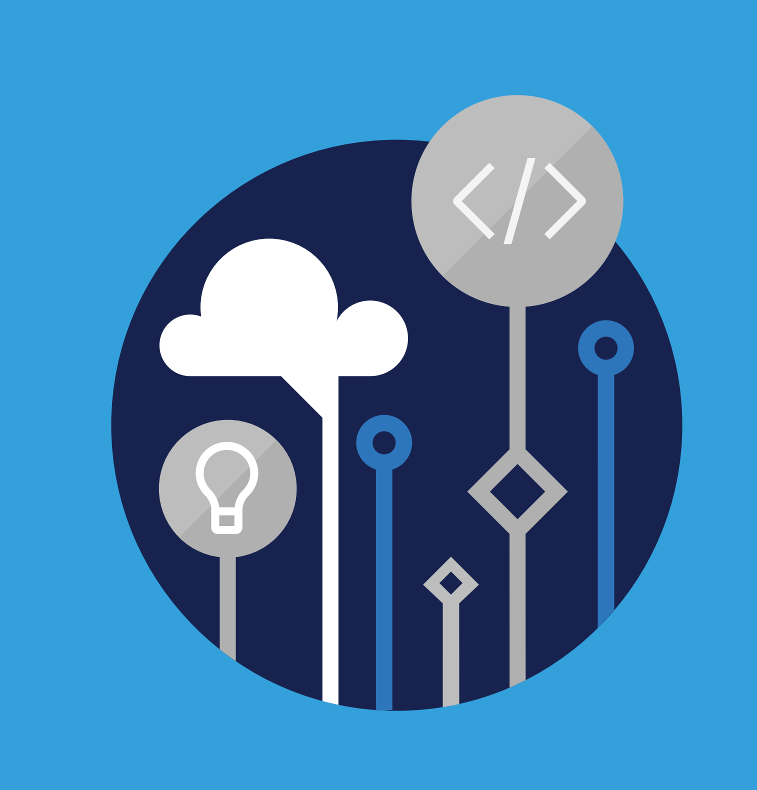


Microsoft Official Course



SC-900T00

Security, Compliance, and Identity Fundamentals

SC-900T00

Security, Compliance, and Identity Fundamentals

1 http://www.microsoft.com/trademarks

MICROSOFT LICENSE TERMS

MICROSOFT INSTRUCTOR-LED COURSEWARE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to your use of the content accompanying this agreement which includes the media on which you received it, if any. These license terms also apply to Trainer Content and any updates and supplements for the Licensed Content unless other terms accompany those items. If so, those terms apply.

BY ACCESSING, DOWNLOADING OR USING THE LICENSED CONTENT, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT ACCESS, DOWNLOAD OR USE THE LICENSED CONTENT.

If you comply with these license terms, you have the rights below for each license you acquire.

1. **DEFINITIONS.**
    1. "Authorized Learning Center" means a Microsoft Imagine Academy (MSIA) Program Member, Microsoft Learning Competency Member, or such other entity as Microsoft may designate from time to time.
    2. "Authorized Training Session" means the instructor-led training class using Microsoft Instructor-Led Courseware conducted by a Trainer at or through an Authorized Learning Center.
    3. "Classroom Device" means one (1) dedicated, secure computer that an Authorized Learning Center owns or controls that is located at an Authorized Learning Center's training facilities that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
    4. "End User" means an individual who is (i) duly enrolled in and attending an Authorized Training Session or Private Training Session, (ii) an employee of an MPN Member (defined below), or (iii) a Microsoft full-time employee, a Microsoft Imagine Academy (MSIA) Program Member, or a Microsoft Learn for Educators – Validated Educator.
    5. "Licensed Content" means the content accompanying this agreement which may include the Microsoft Instructor-Led Courseware or Trainer Content.
    6. "Microsoft Certified Trainer" or "MCT" means an individual who is (i) engaged to teach a training session to End Users on behalf of an Authorized Learning Center or MPN Member, and (ii) currently certified as a Microsoft Certified Trainer under the Microsoft Certification Program.
    7. "Microsoft Instructor-Led Courseware" means the Microsoft-branded instructor-led training course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies. A Microsoft Instructor-Led Courseware title may be branded as MOC, Microsoft Dynamics, or Microsoft Business Group courseware.
    8. "Microsoft Imagine Academy (MSIA) Program Member" means an active member of the Microsoft Imagine Academy Program.
    9. "Microsoft Learn for Educators – Validated Educator" means an educator who has been validated through the Microsoft Learn for Educators program as an active educator at a college, university, community college, polytechnic or K-12 institution.
    10. "Microsoft Learning Competency Member" means an active member of the Microsoft Partner Network program in good standing that currently holds the Learning Competency status.
    11. "MOC" means the "Official Microsoft Learning Product" instructor-led courseware known as Microsoft Official Course that educates IT professionals, developers, students at an academic institution, and other learners on Microsoft technologies.
    12. "MPN Member" means an active Microsoft Partner Network program member in good standing.

13. "Personal Device" means one (1) personal computer, device, workstation or other digital electronic device that you personally own or control that meets or exceeds the hardware level specified for the particular Microsoft Instructor-Led Courseware.
14. "Private Training Session" means the instructor-led training classes provided by MPN Members for corporate customers to teach a predefined learning objective using Microsoft Instructor-Led Courseware. These classes are not advertised or promoted to the general public and class attendance is restricted to individuals employed by or contracted by the corporate customer.
15. "Trainer" means (i) an academically accredited educator engaged by a Microsoft Imagine Academy Program Member to teach an Authorized Training Session, (ii) an academically accredited educator validated as a Microsoft Learn for Educators – Validated Educator, and/or (iii) a MCT.
16. "Trainer Content" means the trainer version of the Microsoft Instructor-Led Courseware and additional supplemental content designated solely for Trainers' use to teach a training session using the Microsoft Instructor-Led Courseware. Trainer Content may include Microsoft PowerPoint presentations, trainer preparation guide, train the trainer materials, Microsoft One Note packs, classroom setup guide and Pre-release course feedback form. To clarify, Trainer Content does not include any software, virtual hard disks or virtual machines.

2. **USE RIGHTS.** The Licensed Content is licensed, not sold. The Licensed Content is licensed on a **one copy per user basis**, such that you must acquire a license for each individual that accesses or uses the Licensed Content.

- 2.1 Below are five separate sets of use rights. Only one set of rights apply to you.

1. **If you are a Microsoft Imagine Academy (MSIA) Program Member:**
    1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
    2. For each license you acquire on behalf of an End User or Trainer, you may either:
        1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User who is enrolled in the Authorized Training Session, and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
        2. provide one (1) End User with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
        3. provide one (1) Trainer with the unique redemption code and instructions on how they can access one (1) Trainer Content.
    3. For each license you acquire, you must comply with the following:
        1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
        2. you will ensure each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
        3. you will ensure that each End User provided with the hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End

User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each Trainer teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified Trainers who have in-depth knowledge of and experience with the Microsoft technology that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Authorized Training Sessions,
6. you will only deliver a maximum of 15 hours of training per week for each Authorized Training Session that uses a MOC title, and
7. you acknowledge that Trainers that are not MCTs will not have access to all of the trainer resources for the Microsoft Instructor-Led Courseware.

2. **If you are a Microsoft Learning Competency Member:**
   1. Each license acquire may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   2. For each license you acquire on behalf of an End User or MCT, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Authorized Training Session and only immediately prior to the commencement of the Authorized Training Session that is the subject matter of the Microsoft Instructor-Led Courseware provided, **or**
      2. provide one (1) End User attending the Authorized Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. you will provide one (1) MCT with the unique redemption code and instructions on how they can access one (1) Trainer Content.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. you will ensure that each End User attending an Authorized Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Authorized Training Session,
      3. you will ensure that each End User provided with a hard-copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,

4. you will ensure that each MCT teaching an Authorized Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Authorized Training Session,
5. you will only use qualified MCTs who also hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Authorized Training Sessions using MOC,
6. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
7. you will only provide access to the Trainer Content to MCTs.

3. **If you are a MPN Member:**
   1. Each license acquired on behalf of yourself may only be used to review one (1) copy of the Microsoft Instructor-Led Courseware in the form provided to you. If the Microsoft Instructor-Led Courseware is in digital format, you may install one (1) copy on up to three (3) Personal Devices. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.
   2. For each license you acquire on behalf of an End User or Trainer, you may either:
      1. distribute one (1) hard copy version of the Microsoft Instructor-Led Courseware to one (1) End User attending the Private Training Session, and only immediately prior to the commencement of the Private Training Session that is the subject matter of the Microsoft Instructor-Led Courseware being provided, **or**
      2. provide one (1) End User who is attending the Private Training Session with the unique redemption code and instructions on how they can access one (1) digital version of the Microsoft Instructor-Led Courseware, **or**
      3. you will provide one (1) Trainer who is teaching the Private Training Session with the unique redemption code and instructions on how they can access one (1) Trainer Content.
   3. For each license you acquire, you must comply with the following:
      1. you will only provide access to the Licensed Content to those individuals who have acquired a valid license to the Licensed Content,
      2. you will ensure that each End User attending an Private Training Session has their own valid licensed copy of the Microsoft Instructor-Led Courseware that is the subject of the Private Training Session,
      3. you will ensure that each End User provided with a hard copy version of the Microsoft Instructor-Led Courseware will be presented with a copy of this agreement and each End User will agree that their use of the Microsoft Instructor-Led Courseware will be subject to the terms in this agreement prior to providing them with the Microsoft Instructor-Led Courseware. Each individual will be required to denote their acceptance of this agreement in a manner that is enforceable under local law prior to their accessing the Microsoft Instructor-Led Courseware,
      4. you will ensure that each Trainer teaching an Private Training Session has their own valid licensed copy of the Trainer Content that is the subject of the Private Training Session,

5. you will only use qualified Trainers who hold the applicable Microsoft Certification credential that is the subject of the Microsoft Instructor-Led Courseware being taught for all your Private Training Sessions,
6. you will only use qualified MCTs who hold the applicable Microsoft Certification credential that is the subject of the MOC title being taught for all your Private Training Sessions using MOC,
7. you will only provide access to the Microsoft Instructor-Led Courseware to End Users, and
8. you will only provide access to the Trainer Content to Trainers.

4. **If you are an End User:**
For each license you acquire, you may use the Microsoft Instructor-Led Courseware solely for your personal training use. If the Microsoft Instructor-Led Courseware is in digital format, you may access the Microsoft Instructor-Led Courseware online using the unique redemption code provided to you by the training provider and install and use one (1) copy of the Microsoft Instructor-Led Courseware on up to three (3) Personal Devices. You may also print one (1) copy of the Microsoft Instructor-Led Courseware. You may not install the Microsoft Instructor-Led Courseware on a device you do not own or control.

5. **If you are a Trainer.**
   1. For each license you acquire, you may install and use one (1) copy of the Trainer Content in the form provided to you on one (1) Personal Device solely to prepare and deliver an Authorized Training Session or Private Training Session, and install one (1) additional copy on another Personal Device as a backup copy, which may be used only to reinstall the Trainer Content. You may not install or use a copy of the Trainer Content on a device you do not own or control. You may also print one (1) copy of the Trainer Content solely to prepare for and deliver an Authorized Training Session or Private Training Session.
   2. If you are an MCT, you may customize the written portions of the Trainer Content that are logically associated with instruction of a training session in accordance with the most recent version of the MCT agreement.
   3. If you elect to exercise the foregoing rights, you agree to comply with the following: (i) customizations may only be used for teaching Authorized Training Sessions and Private Training Sessions, and (ii) all customizations will comply with this agreement. For clarity, any use of "customize" refers only to changing the order of slides and content, and/or not using all the slides or content, it does not mean changing or modifying any slide or content.

- 2.2 **Separation of Components.** The Licensed Content is licensed as a single unit and you may not separate their components and install them on different devices.
- 2.3 **Redistribution of Licensed Content.** Except as expressly provided in the use rights above, you may not distribute any Licensed Content or any portion thereof (including any permitted modifications) to any third parties without the express written permission of Microsoft.
- 2.4 **Third Party Notices.** The Licensed Content may include third party code that Microsoft, not the third party, licenses to you under this agreement. Notices, if any, for the third party code are included for your information only.
- 2.5 **Additional Terms.** Some Licensed Content may contain components with additional terms, conditions, and licenses regarding its use. Any non-conflicting terms in those conditions and licenses also apply to your use of that respective component and supplements the terms described in this agreement.

3. **LICENSED CONTENT BASED ON PRE-RELEASE TECHNOLOGY.** If the Licensed Content's subject matter is based on a pre-release version of Microsoft technology ("**Pre-release**"), then in addition to the other provisions in this agreement, these terms also apply:

   1. **Pre-Release Licensed Content.** This Licensed Content subject matter is on the Pre-release version of the Microsoft technology. The technology may not work the way a final version of the technology will and we may change the technology for the final version. We also may not release a final version. Licensed Content based on the final version of the technology may not contain the same information as the Licensed Content based on the Pre-release version. Microsoft is under no obligation to provide you with any further content, including any Licensed Content based on the final version of the technology.

   2. **Feedback.** If you agree to give feedback about the Licensed Content to Microsoft, either directly or through its third party designee, you give to Microsoft without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft technology, Microsoft product, or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its technology, technologies, or products to third parties because we include your feedback in them. These rights survive this agreement.

   3. **Pre-release Term.** If you are an Microsoft Imagine Academy Program Member, Microsoft Learning Competency Member, MPN Member, Microsoft Learn for Educators – Validated Educator, or Trainer, you will cease using all copies of the Licensed Content on the Pre-release technology upon (i) the date which Microsoft informs you is the end date for using the Licensed Content on the Pre-release technology, or (ii) sixty (60) days after the commercial release of the technology that is the subject of the Licensed Content, whichever is earliest ("**Pre-release term**"). Upon expiration or termination of the Pre-release term, you will irretrievably delete and destroy all copies of the Licensed Content in your possession or under your control.

4. **SCOPE OF LICENSE.** The Licensed Content is licensed, not sold. This agreement only gives you some rights to use the Licensed Content. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Licensed Content only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Licensed Content that only allows you to use it in certain ways. Except as expressly permitted in this agreement, you may not:

   - access or allow any individual to access the Licensed Content if they have not acquired a valid license for the Licensed Content,
   - alter, remove or obscure any copyright or other protective notices (including watermarks), branding or identifications contained in the Licensed Content,
   - modify or create a derivative work of any Licensed Content,
   - publicly display, or make the Licensed Content available for others to access or use,
   - copy, print, install, sell, publish, transmit, lend, adapt, reuse, link to or post, make available or distribute the Licensed Content to any third party,
   - work around any technical limitations in the Licensed Content, or
   - reverse engineer, decompile, remove or otherwise thwart any protections or disassemble the Licensed Content except and only to the extent that applicable law expressly permits, despite this limitation.

5. **RESERVATION OF RIGHTS AND OWNERSHIP.** Microsoft reserves all rights not expressly granted to you in this agreement. The Licensed Content is protected by copyright and other intellectual property

laws and treaties. Microsoft or its suppliers own the title, copyright, and other intellectual property rights in the Licensed Content.

6. **EXPORT RESTRICTIONS.** The Licensed Content is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Licensed Content. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.
7. **SUPPORT SERVICES.** Because the Licensed Content is provided “as is”, we are not obligated to provide support services for it.
8. **TERMINATION.** Without prejudice to any other rights, Microsoft may terminate this agreement if you fail to comply with the terms and conditions of this agreement. Upon termination of this agreement for any reason, you will immediately stop all use of and delete and destroy all copies of the Licensed Content in your possession or under your control.
9. **LINKS TO THIRD PARTY SITES.** You may link to third party sites through the use of the Licensed Content. The third party sites are not under the control of Microsoft, and Microsoft is not responsible for the contents of any third party sites, any links contained in third party sites, or any changes or updates to third party sites. Microsoft is not responsible for webcasting or any other form of transmission received from any third party sites. Microsoft is providing these links to third party sites to you only as a convenience, and the inclusion of any link does not imply an endorsement by Microsoft of the third party site.
10. **ENTIRE AGREEMENT.** This agreement, and any additional terms for the Trainer Content, updates and supplements are the entire agreement for the Licensed Content, updates and supplements.
11. **APPLICABLE LAW.**
    1. United States. If you acquired the Licensed Content in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.
    2. Outside the United States. If you acquired the Licensed Content in any other country, the laws of that country apply.
12. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the Licensed Content. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.
13. **DISCLAIMER OF WARRANTY. THE LICENSED CONTENT IS LICENSED "AS-IS" AND "AS AVAILABLE." YOU BEAR THE RISK OF USING IT. MICROSOFT AND ITS RESPECTIVE AFFILIATES GIVES NO EXPRESS WARRANTIES, GUARANTEES, OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT AND ITS RESPECTIVE AFFILIATES EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.**
14. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT, ITS RESPECTIVE AFFILIATES AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO US$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.**

This limitation applies to

- anything related to the Licensed Content, services, content (including code) on third party Internet sites or third-party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revised April 2019

Contents

Module 0 Course Introduction

About this course

About this course

Course Description

This course provides foundational level knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.

Level:

Beginner

Audience

This course is targeted to those looking to familiarize themselves with the fundamentals of security, compliance, and identity (SCI) across cloud based and related Microsoft services.

This is a broad audience that may include business stakeholders, new or existing IT professionals, or students that have an interest in Microsoft security, compliance, and identity solutions.

The person taking this content should be familiar with Microsoft Azure and Microsoft 365 and wants to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

The content for this course aligns to the SC-900 exam objective domain.

Prerequisites

- General understanding of networking and cloud computing concepts.
- General IT knowledge or any general experience working in an IT environment.
- General understanding of Microsoft Azure and Microsoft 365.

Expected learning

- Describe basic concepts of security, compliance, and identity.
- Describe the concepts and capabilities of Microsoft identity and access management solutions.

- Describe the capabilities of Microsoft security solutions.
- Describe the compliance management capabilities in Microsoft.

Course Syllabus

Module 1 - Describe basic concepts of security, compliance, and identity

Learn about common security and compliance concepts that are foundational to Microsoft solutions. Topics include the shared responsibility and Zero Trust models, encryption, data residency and data sovereignty, and more.

- Lesson 1 - Describe security and compliance concepts.
- Lesson 2 - Describe identity concepts.

Module 2 - Describe the capabilities of Microsoft identity and access management solutions

Azure Active Directory is the tool for identity and access management in the Microsoft Cloud. Learn about Azure AD services and identity principals, secure authentication, access management capabilities, as well as identity protection and governance.

- Lesson 1 - Describe the basic services and identity types of Azure AD.
- Lesson 2 - Describe the authentication capabilities of Azure AD.
- Lesson 3 - Describe the access management capabilities of Azure AD.
- Lesson 4 - Describe the identity protection and governance capabilities of Azure AD.

Module 3 - Describe the capabilities of Microsoft security solutions

Learn about Microsoft's security solutions. Topics covered include network and platform capabilities of Azure, Azure security management with Microsoft Defender for Cloud, and Microsoft Sentinel. You'll learn about threat protection with Microsoft 365 Defender.

- Lesson 1 - Describe the basic security capabilities in Azure.
- Lesson 2 - Describe the security management capabilities of Azure.
- Lesson 3 - Describe the security capabilities of Microsoft Sentinel.
- Lesson 4 - Describe threat protection capabilities with Microsoft 365 Defender

Module 4 - Describe the compliance management capabilities in Microsoft

Learn about Microsoft compliance management through the Service Trust Portal. You'll learn about Microsoft 365 compliance management, information protection and governance, and insider risk solutions. You'll also learn about Azure resource governance capabilities.

- Lesson 1 - Describe the compliance management capabilities of Microsoft.
- Lesson 2 - Describe the compliance management capabilities of Microsoft 365.
- Lesson 3 - Describe the information protection and governance capabilities of Microsoft 365.
- Lesson 4 - Describe the insider risk capabilities in Microsoft 365.
- Lesson 5 - Describe the eDiscovery and audit capabilities of Microsoft 365.
- Lesson 6 - Describe the resource governance capabilities in Azure.

SC-900 Certification Exam

The **SC-900**
Microsoft Security, Compliance, and Identity Fundamentals[1] certification exam is designed for candidates looking to demonstrate foundational level knowledge of security, compliance, and identity (SCI) across cloud-based and related Microsoft services.

This audience is broad and may include business stakeholders, new or existing IT professionals, or students who have an interest in Microsoft security, compliance, and identity solutions.

Candidates should be familiar with Microsoft Azure and Microsoft 365 and want to understand how Microsoft security, compliance, and identity solutions can span across these solution areas to provide a holistic and end-to-end solution.

This exam can be taken as an **optional** first step in learning about Microsoft security, compliance, and identity. While it would be a beneficial first step, validating foundational level knowledge, taking this exam is not a pre-requisite before taking any other Microsoft security-based certifications.

The exam includes four study areas. The percentages indicate the relative weight of each area on the exam. The higher the percentage, the more questions the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.

SC-900 Study Areas	Weights
Describe the Concepts of Security, Compliance, and Identity	10-15%
Describe the capabilities of Microsoft Identity and Access Management Solutions	25-30%
Describe the capabilities of Microsoft Security Solutions	30-35%
Describe the Capabilities of Microsoft Compliance Solutions	25-30%

✓ This exam does not include a hands-on testing component.

1 https://docs.microsoft.com/learn/certifications/exams/sc-900

Module 1 Describe the concepts of security, compliance, and identity

Describe security and compliance concepts

Introduction

As more business data is being accessed from locations outside of the traditional corporate network, security and compliance have become overriding concerns. Organizations need to understand how they can best protect their data, regardless of where it's accessed from, and whether it sits on their corporate network or in the cloud. In addition, organizations need to ensure they're compliant with industry and regulatory requirements to ensure the protection and privacy of data.

This lesson introduces some important security and compliance concepts. You'll learn about the shared responsibility model, defense in depth, and Zero Trust model. You'll be introduced to the concepts of encryption and hashing as ways to protect data. Lastly, you'll learn about concepts that relate to compliance.

After completing this lesson, you'll be able to:

- Describe the shared responsibility and the defense in-depth security models.
- Describe the Zero-Trust model.
- Describe the concepts of encryption and hashing.
- Describe some basic compliance concepts.

Describe the shared responsibility model

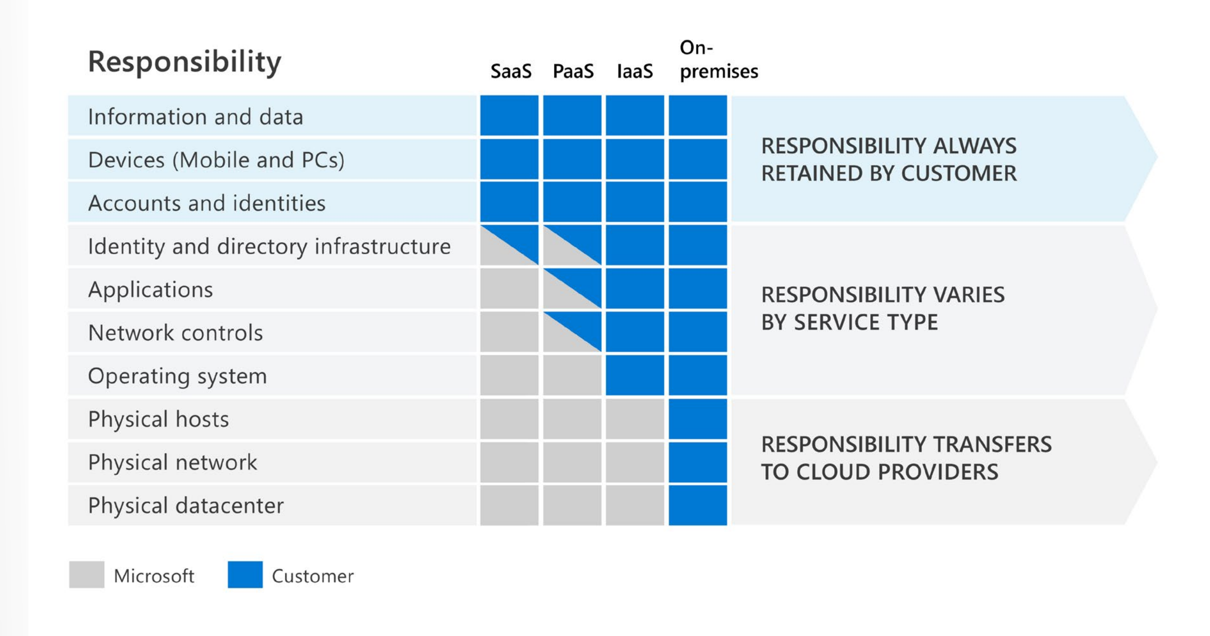
In organizations running only on-premises hardware and software, the organization is 100 percent responsible for implementing security and compliance. With cloud-based services, that responsibility is shared between the customer and the cloud provider.

The *shared responsibility model* identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending on where the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-premises)

The shared responsibility model makes responsibilities clear. When organizations move to the cloud, some responsibilities transfer to the cloud provider and some to the customer organization.

The following diagram illustrates the areas of responsibility between the customer and the cloud provider, according to where data is held.



- **On-premises datacenters (On-premises)**. In an on-premises datacenter, you have responsibility for everything from physical security to encrypting sensitive data.
- **Infrastructure as a Service (IaaS)**. Of all cloud services, IaaS requires the most management by the cloud customer. With IaaS, you're using the cloud provider’s computing infrastructure. The cloud customer isn't responsible for the physical components, such as computers, the network, or the physical security of the datacenter. However, the cloud customer still has responsibility for software components such as operating systems, network controls, applications, and protecting data.
- **Platform as a Service (PaaS)**. PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help you create an application quickly without managing the underlying infrastructure. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

- **Software as a Service (SaaS)**. SaaS is hosted and managed by the cloud provider, for the customer. It's usually licensed through a monthly or annual subscription. Microsoft 365, Skype, and Dynamics CRM Online are all examples of SaaS software. SaaS requires the least amount of management by the cloud customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources.

In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

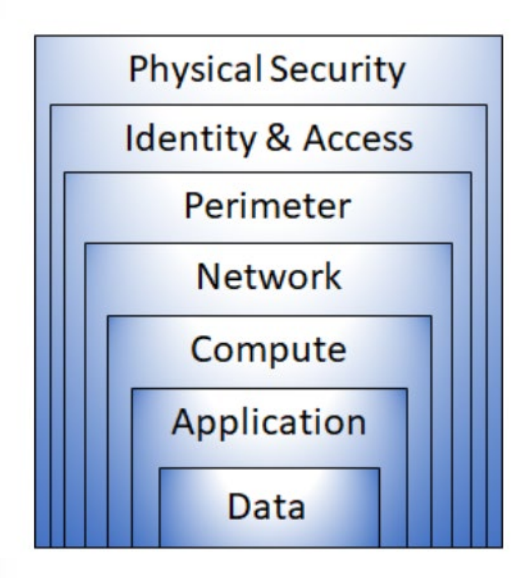
The benefit of the shared responsibility model is that organizations are clear about their responsibilities, and those of the cloud provider.

Describe defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. A defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

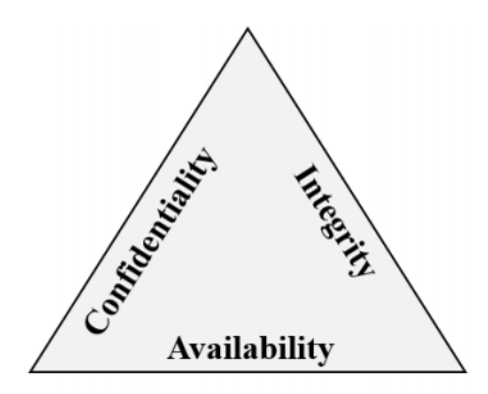
Example layers of security might include:

- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controls, such as multi-factor authentication or condition-based access, to control access to infrastructure and change control.
- **Perimeter** security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security, such as network segmentation and network access controls, to limit communication between resources.
- **Compute** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security to ensure applications are secure and free of security vulnerabilities.
- **Data** layer security including controls to manage access to business and customer data and encryption to protect data.



Confidentiality, Integrity, Availability (CIA)

As described above, a defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. All the different mechanisms (technologies, processes, and training) are elements of a cybersecurity strategy, whose goals include ensuring confidentiality, integrity, and availability; often referred to as CIA.



- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential, but then you also need to keep the encryption keys confidential. Confidentiality is the most visible part of security; we can clearly see need for sensitive data, keys, passwords, and other secrets to be kept confidential.
- **Integrity** refers to keeping data or messages correct. When you send an email message, you want to be sure that the message received is the same as the message you sent. When you store data in a database, you want to be sure that the data you retrieve is the same as the data you stored. Encrypting data keeps it confidential, but you must then be able to decrypt it so that it's the same as before it was encrypted. Integrity is about having confidence that data hasn't been tampered with or altered.
- **Availability** refers to making data available to those who need it, when they need it. It's important to the organization to keep customer data secure, but at the same time it must also be available to employees who deal with customers. While it might be more secure to store the data in an encrypted format, employees need access to decrypted data.

While the goals of a cybersecurity strategy are to preserve the confidentiality, integrity, and availability of systems, networks, applications, and data; it's the goal of cybercriminals to disrupt these goals. Microsoft's portfolio includes the solutions and technologies to enable organizations to deliver on the goals of the CIA triad.

Describe the Zero-Trust model

Zero Trust assumes everything is on an open and untrusted network, even resources behind the firewalls of the corporate network. The Zero Trust model operates on the principle of "**trust no one, verify everything.**"

Attackers' ability to bypass conventional access controls is ending any illusion that traditional security strategies are sufficient. By no longer trusting the integrity of the corporate network, security is strengthened.

In practice, this means that we no longer assume that a password is sufficient to validate a user but add multi-factor authentication to provide additional checks. Instead of granting access to all devices on the corporate network, users are allowed access only to the specific applications or data that they need.

Zero Trust guiding principles

The Zero Trust model has three principles which guide and underpin how security is implemented. These are: verify explicitly, least privilege access, and assume breach.

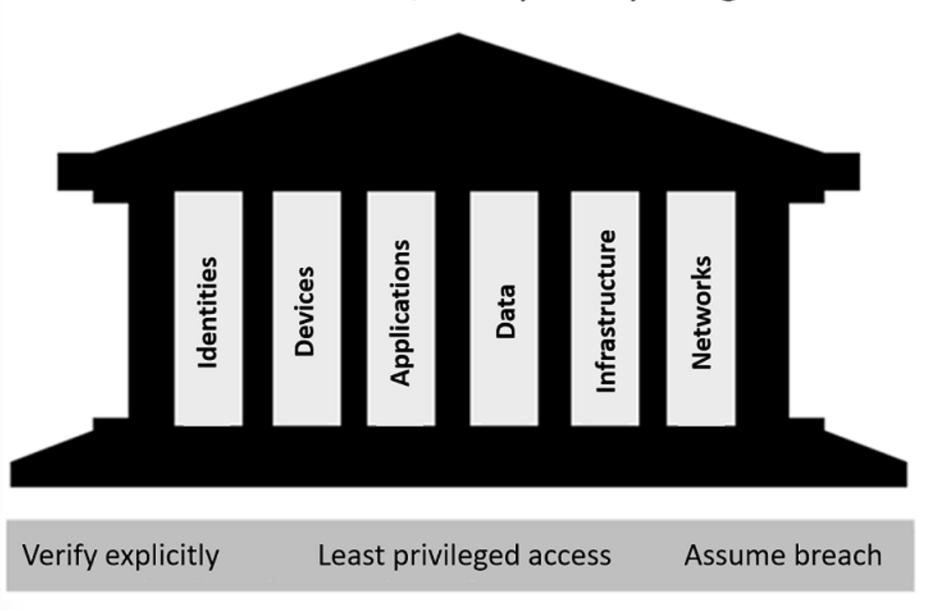
- **Verify explicitly**. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
- **Least privileged access**. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- **Assume breach**. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

Six foundational pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- **Identities** may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication, and follow least privilege access principles.
- **Devices** create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- **Applications** are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- **Data** should be classified, labeled, and encrypted based on its attributes. Security efforts are ultimately about protecting data, and ensuring it remains safe when it leaves devices, applications, infrastructure, and networks that the organization controls.
- **Infrastructure**, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies. This allows you to automatically block or flag risky behavior and take protective actions.

- **Networks** should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.



A security strategy that employs the three principles of the Zero Trust model across the six foundational pillars helps companies deliver and enforce security across their organization.

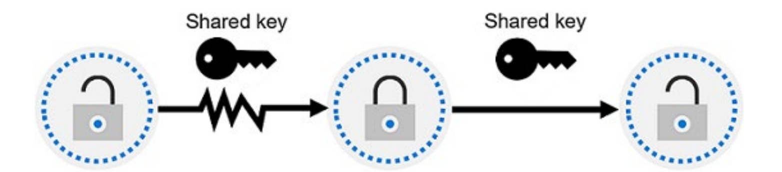
Refer to **An introduction to the Zero Trust methodology**[1] for a video recap on the pillars of the Zero Trust model.

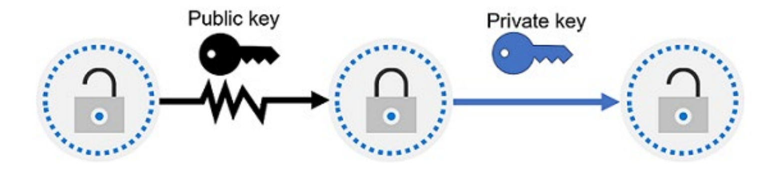
Describe encryption and hashing

One way to mitigate against common cybersecurity threats is to encrypt sensitive or valuable data. Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

There are two top-level types of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt the data. Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, you need a paired key. Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions. Encryption may protect data at rest, or in transit.

1 https://www.microsoft.com/videoplayer/embed/RE4J3ms





Encryption for data at rest

Data at rest is the data that's stored on a physical device, such as a server. It may be stored in a database or a storage account but, regardless of where it's stored, encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

If an attacker obtained a hard drive with encrypted data and didn't have access to the encryption keys, they would be unable to read the data.

Encryption for data in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encrypting data in transit protects it from outside observers and provides a mechanism to transmit data while limiting the risk of exposure.

Encryption for data in use

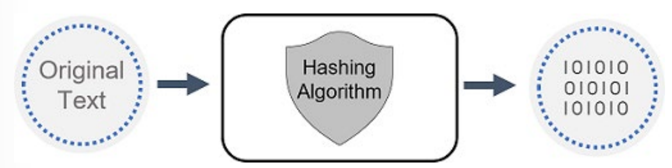
A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

Hashing

Hashing uses an algorithm to convert text to a *unique* fixed-length value called a hash. Each time the same text is hashed using the same algorithm, the same hash value is produced. That hash can then be used as a unique identifier of its associated data.

Hashing is different to encryption in that it doesn't use keys, and the hashed value isn't subsequently decrypted back to the original.

Hashing is used to store passwords. When a user enters their password, the same algorithm that created the stored hash creates a hash of the entered password. This is compared to the stored hashed version of the password. If they match, the user has entered their password correctly. This is more secure than storing plain text passwords, but hashing algorithms are also known to hackers. Because hash functions are deterministic (the same input produces the same output), hackers can use brute-force dictionary attacks by hashing the passwords. For every matched hash, they know the actual password. To mitigate this risk, passwords are often “salted”. This refers to adding a fixed-length random value to the input of hash functions to create unique hashes for same input.



Describe compliance concepts

Data has become more important than ever. Organizations, institutions, and entire societies generate and rely on data to function on a day-to-day basis. The sheer scale of data generated and the increasing reliance on it means that the privacy and protection of that data has become pivotal. As organizations and institutions move their data to service provider clouds, with datacenters all over the world, additional considerations come into play.

Government agencies and industry groups have issued regulations to help protect and govern the use of data. From personal and financial information to data protection and privacy, organizations can be accountable for meeting dozens of regulations to be compliant. Listed below are some important concepts and terms that relate to data compliance.

- **Data residency** - When it comes to compliance, data residency regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally. These regulations can differ significantly depending on jurisdiction.
- **Data sovereignty** - Another important consideration is data sovereignty, the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed. This can add a layer of complexity when it comes to compliance because the same piece of data can be collected in one location, stored in another, and processed in still another; making it subject to laws from different countries/regions.
- **Data privacy** - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations. Personal data means any information relating to an identified or identifiable natural person. Privacy laws previously referenced “PII” or "personally identifiable information" but the laws have expanded the definition to any data that is directly linked or indirectly linkable back to a person. Organizations are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards governing data privacy.

In most cases, laws and regulations don't define or prescribe specific technologies that organizations must use to protect data. They leave it to an organization to identify compliant technologies, operations, and other appropriate data-protection measures.

Knowledge check

Multiple choice

Item 1. An organization has deployed Microsoft 365 applications to all employees. Considering the shared responsibility model, who is responsible for the accounts and identities relating to these employees?

- ☐ The organization.
- ☐ Microsoft, the SaaS provider.
- ☐ The shared responsibility between your organization and Microsoft.

Multiple choice

Item 2. Which of the following measures might an organization implement as part of the defense in-depth security methodology?

- ☐ Locating all its servers in a single physical location.
- ☐ Multi-factor authentication for all users.
- ☐ Ensuring there's no segmentation of your corporate network.

Multiple choice

Item 3. The human resources organization wants to ensure that stored employee data is encrypted. Which security mechanism would they use?

- ☐ Hashing.
- ☐ Encryption in transit.
- ☐ Encryption at rest.

Multiple choice

Item 4. Which of the following best describes the concept of data sovereignty?

- ☐ There are regulations that govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally.
- ☐ Data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.
- ☐ Trust no one, verify everything.

Summary and resources

In this lesson you were introduced to some important security and compliance concepts. You learned about the shared responsibility model and how the workload responsibilities vary depending on where the workload is hosted. You learned how a defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. You learned about the guiding principles of Zero Trust and how the six foundational pillars work together to enforce organization security policies. Lastly, you were introduced to the concepts of encryption and hashing as ways to secure your data and some basic concepts related to data compliance.

Now that you've completed this lesson, you should be able to:

- Describe the shared responsibility and the defense in-depth security models.
- Describe the Zero-Trust model.
- Describe the concepts of encryption and hashing.
- Describe some basic compliance concepts.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Zero Trust Resource Center**[2]
- **Shared responsibility in the cloud**[3]
- **Azure defense in depth**[4]
- **Enabling Data Residency and Data Protection in Microsoft Azure Regions**[5]

2 https://docs.microsoft.com/security/zero-trust/
3 https://docs.microsoft.com/azure/security/fundamentals/shared-responsibility
4 https://azure.microsoft.com/resources/videos/defense-in-depth-security-in-azure/
5 https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling_Data_Residency_and_Data_Protection_in_Azure_Regions-2021.pdf

Describe identity concepts

Introduction

Everyone, and every device, has an identity that can be used to access resources. Identity is the way in which people and things are identified on your corporate network, and in the cloud. Being certain about who or what is accessing your organization's data and other resources is a fundamental part of securing your environment.

In this lesson, you'll learn about the key concepts of authentication and authorization and why identity is important in securing corporate resources. You'll also learn about some identity related services.

After completing this lesson, you'll be able to:

- Understand the difference between authentication and authorization.
- Describe the concept of identity as a security perimeter.
- Describe identity-related services.

Define authentication and authorization

A key concept associated with identity is the concept of authentication and authorization and understanding what they do and how they're different.

Authentication

Authentication is the process of proving that a person is who they say they are. When someone purchases an item with a credit card, they may be required to show an additional form of identification. This proves that they are the person whose name appears on the card. In this example, the user may show a driver's license that serves as a form of authentication and proves their ID.

When you want to access a computer or device, you'll encounter a similar type of authentication. You may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password, together, are a form of authentication. Authentication is sometimes shortened to AuthN.

Authorization

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization.

Suppose you want to spend the night in a hotel. The first thing you'll do is go to reception to start the "authentication process". After the receptionist has verified who you are, you're given a keycard and can go to your room. Think of the keycard as the authorization process. The keycard will only let you open the doors and elevators you're permitted to access, such as for your hotel room.

In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to AuthZ.

Define Identity as the primary security perimeter

Digital collaboration has changed. Your employees and partners now need to collaborate and access organizational resources from anywhere, on any device, and without affecting their productivity. There has also been an acceleration in the number of people working from home.

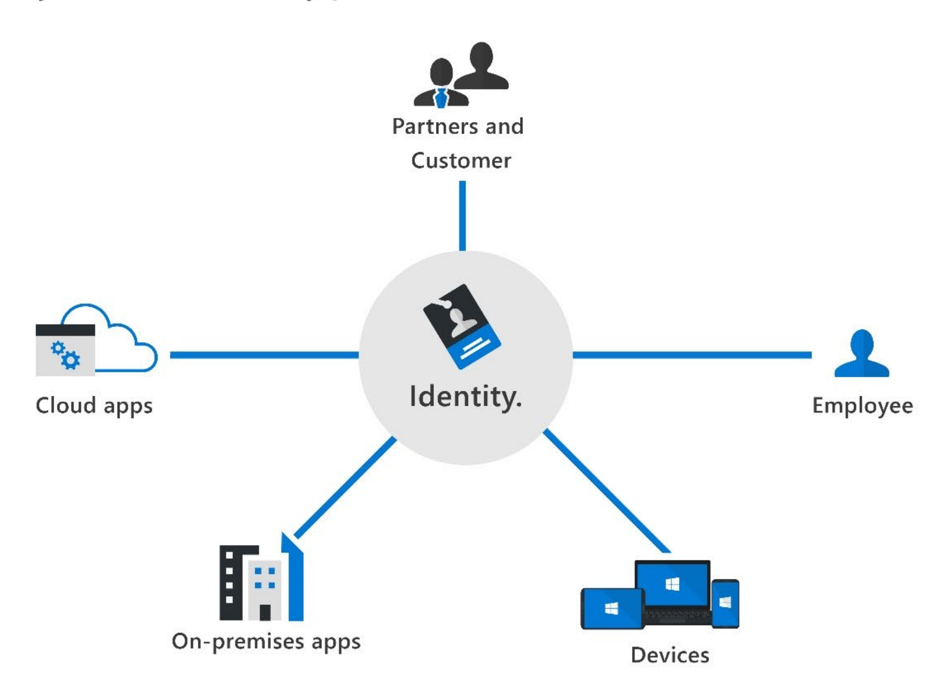
Enterprise security needs to adapt to this new reality. The security perimeter can no longer be viewed as the on-premises network. It now extends to:

- SaaS applications for business-critical workloads that might be hosted outside the corporate network.
- The personal devices that employees are using to access corporate resources (BYOD, or bring your own device) while working from home.
- The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees
- Internet of things, referred to as IoT devices, installed throughout your corporate network and inside customer locations.

The traditional perimeter-based security model is no longer enough. Identity has become the new security perimeter that enables organizations to secure their assets.

But what do we mean by an identity? An identity is the set of things that define or characterize someone or something. For example, a person's identity includes the information they use to authenticate themselves, such, as their username and password and their level of authorization.

An identity may be associated with a user, an application, a device, or something else.



Four pillars of an identity infrastructure

Identity is a concept that spans an entire environment, so organizations need to think about it broadly. There's a collection of processes, technologies, and policies for managing digital identities and controlling how they're used to access resources. These can be organized into four fundamental pillars that organizations should consider when creating an identity infrastructure.

- **Administration**. Administration is about the creation and management/governance of identities for users, devices, and services. As an administrator, you manage how and under what circumstances the characteristics of identities can change (be created, updated, deleted).
- **Authentication**. The authentication pillar tells the story of how much an IT system needs to know about an identity to have sufficient proof that they really are who they say they are? It involves the act of challenging a party for legitimate credentials.
- **Authorization**. The authorization pillar is about processing the incoming identity data to determine the level of access an authenticated person or service has within the application or service that it wants to access.
- **Auditing**. The auditing pillar is about tracking who does what, when, where, and how. Auditing includes having in-depth reporting, alerts, and governance of identities.

Addressing each of these four pillars is key to a comprehensive and robust identity and access control solution.

Describe the role of the identity provider

Modern authentication is an umbrella term for authentication and authorization methods between a client, such as your laptop or phone, and a server, like a website or application. At the center of modern authentication is the role of the *identity provider*. An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.

With modern authentication, all services, including all authentication services, are supplied by a central identity provider. Information that's used to authenticate the user with the server is stored and managed centrally by the identity provider.

With a central identity provider, organizations can establish authentication and authorization policies, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

For information about modern authentication and how it works with a central identity provider watch **Azure Active Directory: Authentication fundamentals - The basics**[6].

In a client-server scenario using modern authentication (as described in the video), the client communicates with the identity provider by providing an identity which can be authenticated. Once the identity (which can be a user or an application) has been verified, the identity provider issues a *security token* which the client sends to the server. The server validates the security token through its *trust relationship* with the identity provider. By using the security token and the information that is contained within the token, the user or application can gain access to the required resources on the server. In this scenario, the token and the information contained in the token is stored and managed by the identity provider. The centralized identity provider is providing the authentication service.

Microsoft Azure Active Directory is an example of a cloud-based identity provider. Other examples of identity providers include Twitter, Google, Amazon, LinkedIn, and GitHub.

6 https://www.microsoft.com/videoplayer/embed/RE4Kdt9

Single sign-on

Another fundamental capability of an identity provider and "modern authentication" is the support for single sign-on (SSO). With SSO, the user logs in once and that credential is used to access multiple applications or resources.
When you set up single sign-on to work between multiple identity providers, it's called federation.

Describe the concept of directory services and Active Directory

In the context of a computer network, a directory is a hierarchical structure that stores information about objects on the network. A directory service stores directory data and makes it available to network users, administrators, services, and applications.

Active Directory (AD) is a set of directory services developed by Microsoft as part of Windows 2000 for on-premises domain-based networks. The best-known service of this kind is Active Directory Domain Services (AD DS). It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights. A server running AD DS is a domain controller (DC).

AD DS is a central component in organizations with on-premises IT infrastructure. AD DS gives organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. AD DS doesn't, however, natively support mobile devices, SaaS applications, or line of business apps that require *modern authentication* methods.

The growth of cloud services, SaaS applications, and personal devices being used at work, has resulted in the need for modern authentication, and an evolution of Active Directory-based identity solutions.

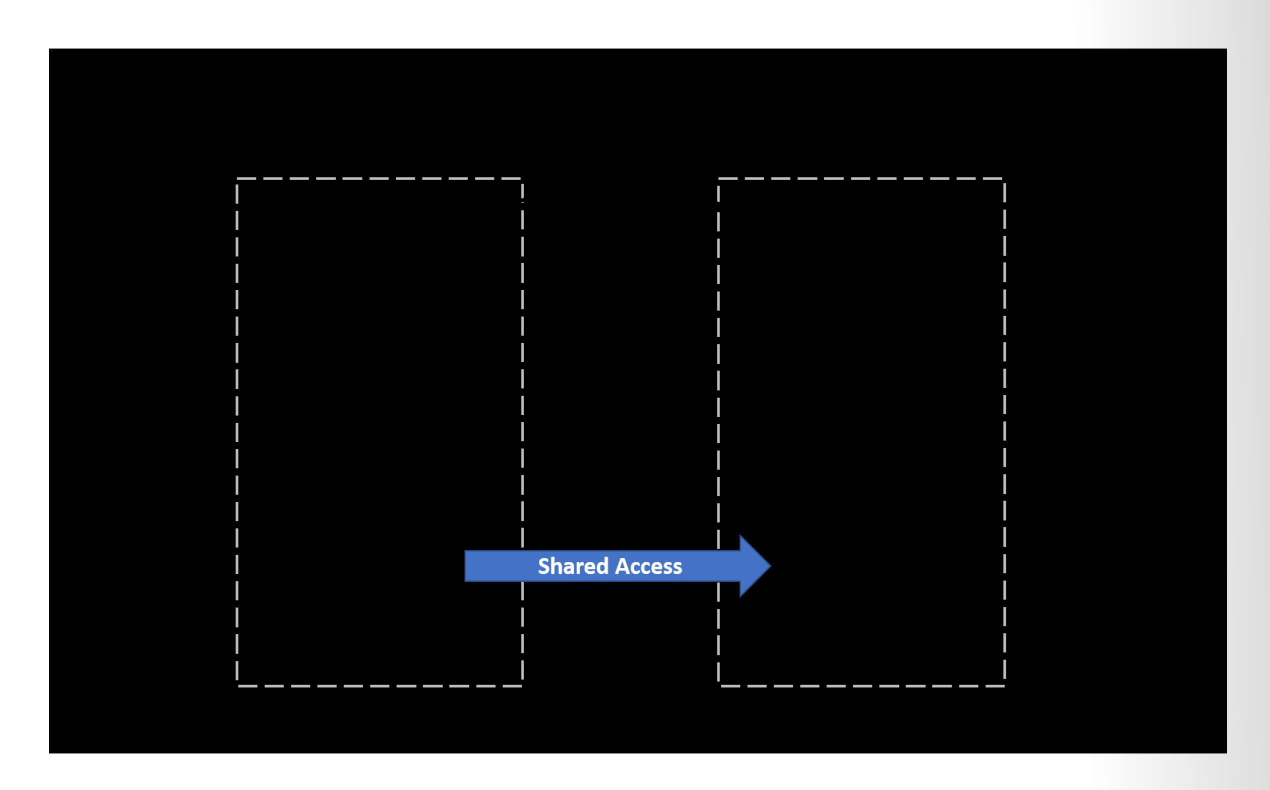
Azure Active Directory is the next evolution of identity and access management solutions. It provides organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.
In this course, we'll focus on Azure AD, Microsoft's cloud-based identity provider.

To learn more visit **Compare Active Directory to Azure Active Directory**[7].

Describe the concept of Federation

Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider. With federation, there's no need for a user to maintain a different username and password when accessing resources in other domains.

7 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad



The simplified way to think about this federation scenario is as follows:

- The website, in domain A, uses the authentication services of Identity Provider A (IdP-A).
- The user, in domain B, authenticates with Identity Provider B (IdP-B).
- IdP-A has a trust relationship configured with IdP-B.
- When the user, who wants to access the website, provides his/her credentials to the website, the website trusts the user and allows access. This access is allowed because of the trust that is already established between the two identity providers.

With federation, trust isn't always bidirectional. Although IdP-A may trust IdP-B and allow the user in domain B to access the website in domain A, the opposite isn't true, unless that trust relationship is configured.

A common example of federation in practice is when a user logs in to a third-party site with their social media account, such as Twitter. In this scenario, Twitter is an identity provider, and the third-party site might be using a different identity provider, such as Azure AD. There's a trust relationship between Azure AD and Twitter.

Knowledge check

Multiple choice

Item 1. What is a benefit of single sign-on?

☐ A central identity provider can be used.

☐ The user signs in once and then can access many applications or resources.

☐ Passwords always expire after 72 days.

Multiple choice

Item 2. Which relationship allows federated services to gain access to resources?

- ☐ Claim relationship.
- ☐ Shared access relationship.
- ☐ Trust relationship.

Multiple choice

Item 3. Authentication is the process of doing what?

- ☐ Verifying that a user or device is who they say they are.
- ☐ The process of profiling user behavior.
- ☐ Enabling federated services.

Summary and resources

In this lesson, you learned about authentication and authorization. You've learned about identity as the new security perimeter and the role of Active Directory. You also looked at the concept of federation to access resources that belong to another organization.

Now you've completed this lesson, you'll be able to:

- Understand the difference between authentication and authorization.
- Describe the concept of identity as a security perimeter.
- Describe identity-related services.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Authentication vs authorization**[8]
- **Identity providers for External Identities**[9]
- **Compare Active Directory to Azure Active Directory**[10]

8 https://docs.microsoft.com/azure/active-directory/develop/authentication-vs-authorization
9 https://docs.microsoft.com/azure/active-directory/external-identities/identity-providers
10 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

Answers

Multiple choice

Item 1. An organization has deployed Microsoft 365 applications to all employees. Considering the shared responsibility model, who is responsible for the accounts and identities relating to these employees?

■ The organization.

☐ Microsoft, the SaaS provider.

☐ The shared responsibility between your organization and Microsoft.

Explanation
In the shared responsibility model, the customer organization always has responsibility for their data, including information and data relating to employees, devices, and accounts and identities.

Multiple choice

Item 2. Which of the following measures might an organization implement as part of the defense in-depth security methodology?

☐ Locating all its servers in a single physical location.

■ Multi-factor authentication for all users.

☐ Ensuring there's no segmentation of your corporate network.

Explanation
Multi-factor authentication is an example of defense in-depth at the identity and access layer.

Multiple choice

Item 3. The human resources organization wants to ensure that stored employee data is encrypted. Which security mechanism would they use?

☐ Hashing.

☐ Encryption in transit.

■ Encryption at rest.

Explanation
Encryption at rest could be part of a security strategy to protect stored employee training data.

Multiple choice

Item 4. Which of the following best describes the concept of data sovereignty?

☐ There are regulations that govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally.

■ Data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.

☐ Trust no one, verify everything.

Explanation
Data sovereignty is the concept that data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.

Multiple choice

Item 1. What is a benefit of single sign-on?

☐ A central identity provider can be used.

■ The user signs in once and then can access many applications or resources.

☐ Passwords always expire after 72 days.

Explanation
With single sign-on a user signs in once and can then access a number of applications or resources.

Multiple choice

Item 2. Which relationship allows federated services to gain access to resources?

☐ Claim relationship.

☐ Shared access relationship.

■ Trust relationship.

Explanation
Federated services use a trust relationship to allow access to resources.

Multiple choice

Item 3. Authentication is the process of doing what?

■ Verifying that a user or device is who they say they are.

☐ The process of profiling user behavior.

☐ Enabling federated services.

Explanation
Authentication is the process of verifying that a user or device is who they say they are.

Module 2 Describe the capabilities of Microsoft identity and access management solutions

Describe the basic services and identity types of Azure AD

Introduction

When it comes to security, your organization can no longer rely on its network boundary. To allow employees, partners, and customers to collaborate securely, organizations need to shift to an approach whereby identity becomes the new security perimeter. Using an identity provider helps organizations manage that shift and all the aspects of identity security.

This lesson introduces you to Azure Active Directory (Azure AD), Microsoft's cloud-based identity and access management service. In this module, you'll learn about the benefits of using a cloud-based identity provider, including single sign-on for users. You'll also find out about the different Azure AD editions, the identity types supported by Azure AD, and how you can use it to support external users.

After completing this lesson, you'll be able to:

- Describe what Azure AD does.
- Describe the identity types that Azure AD supports.

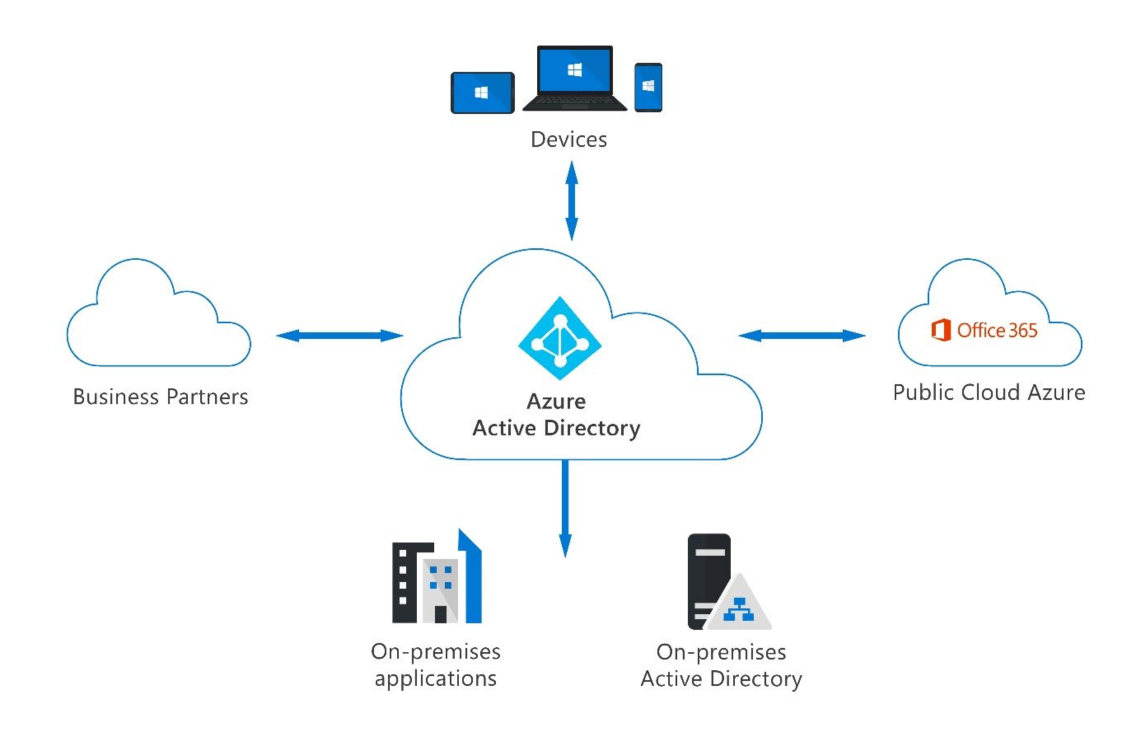
Describe Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. Organizations use Azure AD to enable their employees, guests, and others to sign in and access the resources they need, including:

- Internal resources, such as apps on your corporate network and intranet, and cloud apps developed by your own organization.
- External services, such as Microsoft Office 365, the Azure portal, and any SaaS applications used by your organization.

Azure AD simplifies the way organizations manage authorization and access by providing a single identity system for their cloud and on-premises applications. Azure AD can be synchronized with your existing on-premises Active Directory, synchronized with other directory services, or used as a standalone service.

Azure AD also allows organizations to securely enable the use of personal devices, such as mobiles and tablets, and enable collaboration with business partners and customers.



Azure AD is used by IT admins to control access to corporate apps and resources, based on business requirements. It can also be set up to require multi-factor authentication when accessing important organizational resources. Azure AD can be used to automate user provisioning between an existing Windows Server AD and cloud apps, including Microsoft 365. Finally, Azure AD provides powerful tools to automatically help protect user identities and credentials and to meet an organization's access governance requirements.

Developers use Azure AD as a standards-based approach for adding single sign-on (SSO) to their apps, so that users can sign in with their pre-existing credentials. Azure AD also provides APIs that allow developers to build personalized app experiences using existing organizational data.

Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Azure AD. Users of these services can take advantage of included Azure AD services and can also enhance their Azure AD implementation by upgrading to Azure AD Premium licenses.

Azure AD is available in four editions: Free, Office 365 Apps, Premium P1, and Premium P2. For more information on what is included with each of these editions, refer to **Azure Active Directory Pricing**[1].

1 https://azure.microsoft.com/pricing/details/active-directory/

Describe the Azure AD identity types

Azure AD manages different types of identities: users, service principals, managed identities, and devices. In this unit, we consider each type of Azure AD identity.

User

A user identity is a representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD. If you have several users with the same access needs, you can create a group. You use groups to give access permissions to all members of the group, instead of having to assign access rights individually.

Azure AD business-to-business (B2B) collaboration, a feature within External Identities, includes the capability to add guest users. With B2B collaboration, an organization can securely share applications and services with guest users from another organization.

In the following interactive guide, you'll add a new user to Azure Active Directory. Select the link below to get started and follow the prompts on the screen.

Interactive guide - Add a new user to Azure Active Directory[2]

Service principal

A service principal is, essentially, an identity for an application. For an application to delegate its identity and access functions to Azure AD, the application must first be registered with Azure AD to enable its integration. Once registered, a service principal is created in each Azure AD tenant where the application is used. The service principal enables core features such as authentication and authorization of the application to resources that are secured by the Azure AD tenant.

For the service principals to be able to access resources secured by the Azure AD tenant, application developers must manage and protect the credentials.

Managed identity

Managed identities are a type of service principal that are automatically managed in Azure AD and eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to Azure resources that support Azure AD authentication and can be used without any extra cost.

2 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP02M02-Create-a-New-User-in-Azure-Active-Directory/index.html?azure-portal=true

I can use Managed Identities when…

As a developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure Storage
….

that accesses

Target:

Any target that supports Azure Active Directory Authentication:
- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL…

without having to manage any credentials!

For example, I want to build an application using ***Azure App Services*** that accesses **Azure Storage** without having to manage any credentials.

For a list of Azure Services that support managed identities, refer to **Azure Services that support managed identities**[3].

There are two types of managed identities: system-assigned and user-assigned.

System-assigned. Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity, an identity is created in Azure AD that's tied to the lifecycle of that service instance. When the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.

User-assigned. You may also create a managed identity as a standalone Azure resource. Once you create a user-assigned managed identity, you can assign it to one or more instances of an Azure service. With user-assigned managed identities, the identity is managed separately from the resources that use it.

The following table summarizes the differences between system-assigned and user-assigned managed identities:

Property	System-assigned managed identity	User-assigned managed identity
Creation	Created as part of an Azure resource, such as an Azure virtual machine or Azure App Service.	Created as a standalone Azure resource.
Lifecycle	Shared lifecycle with the Azure resource. When the parent resource is deleted, the managed identity is also deleted.	Independent life cycle. Must be explicitly deleted.
Sharing across Azure resources	Cannot be shared. Associated with a single Azure resource.	Can be shared. A user-assigned managed identity can be associated with more than one Azure resource.

3 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities

Property	System-assigned managed identity	User-assigned managed identity
Common use cases	Workloads that are contained within a single Azure resource. Workloads for which you need independent identities, such as an application that runs on a single virtual machine.	Workloads that run on multiple resources and which can share a single identity. Workloads that need preauthorization to a secure resource as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource.

Device

A device is a piece of hardware, such as mobile devices, laptops, servers, or printers. A device identity gives administrators information they can use when making access or configuration decisions. Device identities can be set up in different ways in Azure AD.

- **Azure AD registered devices**. The goal of Azure AD registered devices is to provide users with support for bring your own device (BYOD) or mobile device scenarios. In these scenarios, a user can access your organization's resources using a personal device. Azure AD registered devices register to Azure AD without requiring an organizational account to sign in to the device. Supported operating systems for Azure AD registered devices include Windows 10 and above, iOS, Android, and macOS.
- **Azure AD joined**. An Azure AD joined device is a device joined to Azure AD through an organizational account, which is then used to sign in to the device. Azure AD joined devices are generally owned by the organization. Supported operating systems for Azure AD joined devices include Windows 10 or greater (except Home edition) and Windows Server 2019 Virtual Machines running in Azure.
- **Hybrid Azure AD joined devices**. Organizations with existing on-premises Active Directory implementations can benefit from the functionality provided by Azure AD by implementing hybrid Azure AD joined devices. These devices are joined to your on-premises Active Directory and Azure AD requiring organizational account to sign in to the device

Registering and joining devices to Azure AD gives users Single Sign-on (SSO) to cloud-based resources. Additionally, devices that are Azure AD joined benefit from the SSO experience to resources and applications that rely on on-premises Active Directory.

IT admins can use tools like Microsoft Intune, a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM), to control how an organization's devices are used. Refer to **Microsoft Intune**[4] for more information.

Describe the types external identities

Today's world is about collaboration, working with people both inside and outside of your organization. That means you'll sometimes need to provide access to your organization's applications or data to external users.

4 https://docs.microsoft.com/mem/intune/fundamentals/what-is-intune

Azure AD External Identities is a set of capabilities that enable organizations to allow access to external users, such as customers or partners. Your customers, partners, and other guest users can “bring their own identities” to sign in.

This ability for external users is enabled through Azure AD support of external identity providers like other Azure AD tenants, Facebook, Google, or enterprise identity providers. Admins can set up federation with identity providers so your external users can sign in with their existing social or enterprise accounts instead of creating a new account just for your application.

There are two different Azure AD External Identities: B2B and B2C.

- B2B collaboration allows you to share your apps and resources with external users.
- B2C is an identity management solution for consumer and customer facing apps.

B2B collaboration

B2B collaboration allows you to share your organization’s applications and services with guest users from other organizations, while maintaining control over your own data. B2B collaboration uses an invitation and redemption process. You can also enable self-service sign-up user flows to let external users sign up for apps or resources themselves. Once the external user has redeemed their invitation or completed sign-up, they're represented in the same directory as employees but with a user type of guest. As a guest, they can now access your resources with their credentials.

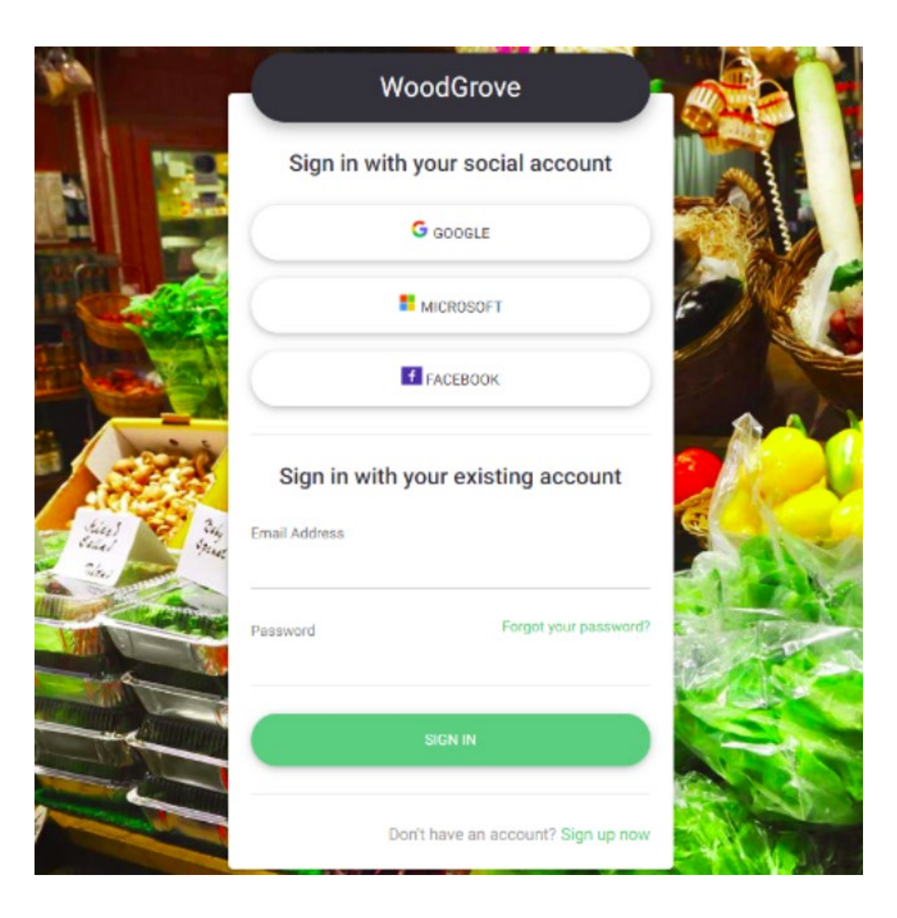
Guest users can be managed in the same way as employees, added to the same groups, and so on. With B2B, SSO to all Azure AD-connected apps are supported.

B2C access management

Azure AD B2C is a customer identity access management (CIAM) solution. Azure AD B2C allows external users to sign in with their preferred social, enterprise, or local account identities to get single sign-on to your applications. Azure AD B2C supports millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

With Azure AD B2C, external users are managed in the Azure AD B2C directory, separately from the organization's employee and partner directory. SSO to customer owned apps within the Azure AD B2C tenant is also supported.

Azure AD B2C is an authentication solution that you can customize with your brand so that it blends with your web and mobile applications.



Azure AD External Identities is a feature of Premium P1 and P2 Azure AD editions, and pricing is based on Monthly Active Users. Refer to **Azure AD pricing** [5] for more details.

Describe the concept of hybrid identities

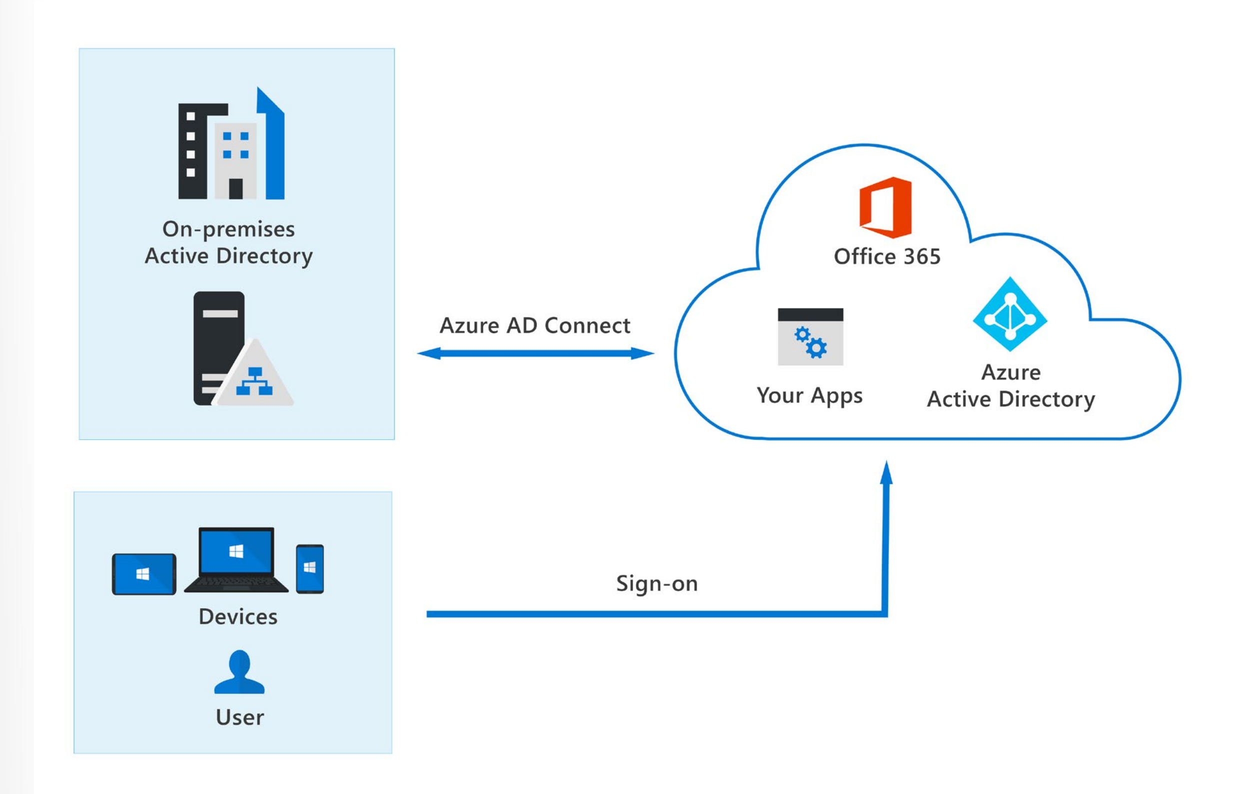
Many organizations are a mixture of both cloud and on-premises applications. Regardless of whether an application is hosted on-premises or in the cloud, users expect and require easy access.
Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this **hybrid identity**.

An important consideration for organizations that operate in a mixed cloud and on-premises environment (hybrid model) is determining the right authentication method for their Azure AD solution, for their organization. This is an important decision in an organization's journey to the cloud and how users will sign in and access applications. It's the foundation for the organization's modern IT infrastructure on top of which organizations will build their security, identity, and access management solution using Azure AD. Lastly, once an authentication method is established it becomes more difficult to change because it can disrupt users' sign-in experience.
When it comes to authentication of hybrid identities, Microsoft offers several ways to authenticate.

- Azure AD Password hash synchronization.
- Azure AD Pass-through authentication
- Federated authentication

5 https://azure.microsoft.com/pricing/details/active-directory/external-identities/

These hybrid authentication options, described below, require an on-premises active directory. Additionally, Azure AD Connect, an on-premises Microsoft application that runs on a server, is required, and serves as a bridge between Azure AD and the on-premises Active Directory.



Azure AD Password hash synchronization. Azure AD password hash synchronization is the simplest way to enable authentication for on-premises directory objects in Azure AD. Users can sign in to Azure AD services by using the same username and password that they use to sign in to their on-premises Active Directory instance. Azure AD handles users' sign-in process.

The Active Directory domain service (AD DS) stores passwords in the form of a hash value representation, of the actual user password. With Azure AD password hash synchronization, the password hash is extracted from the on-premises Active Directory instance using Azure AD Connect. Some extra security is applied to the password hash and then it's synchronized to the Azure Active Directory authentication service. When a user attempts to sign into Azure AD and enters their password, the password is run through the same hashing algorithm and additional security that was applied to the version stored in Azure AD, as part of the synchronization. If the result matches the hash value stored in Azure AD, the user has entered the correct password and is authenticated.

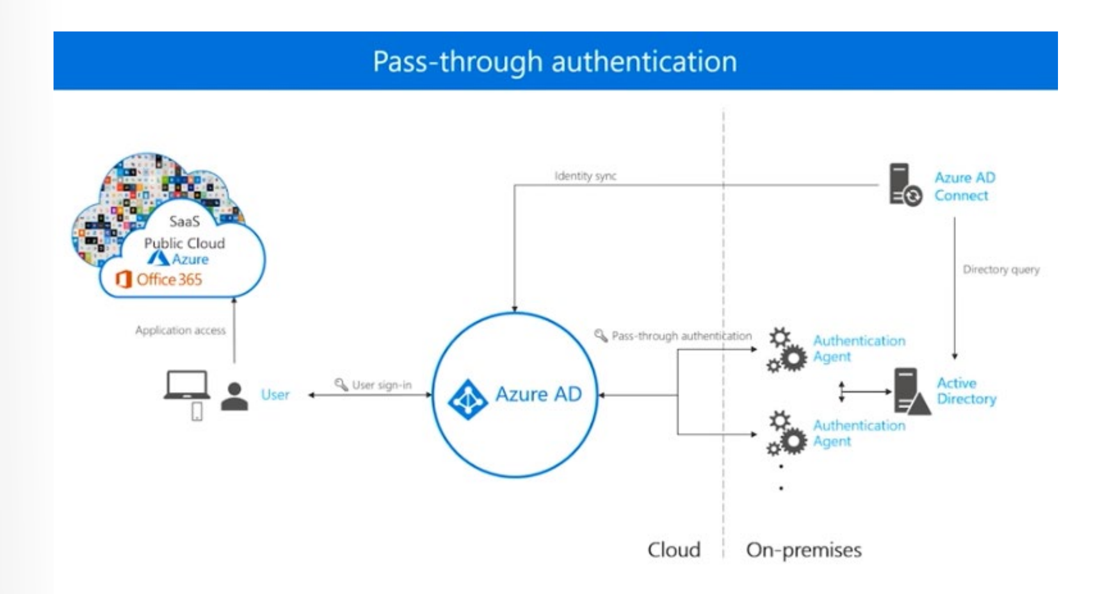
With password hash synchronization, Azure AD Connect ensures that password hash is sync'ed between the on-premises Active Directory and Azure AD. This enables user authentication to take place against Azure AD rather than against the organization's own Active Directory instance. A benefit of this approach is that password hash synchronization provides highly available cloud authentication. On-premise users can authenticate with Azure AD to access cloud-based applications, even if the on-premise Active Directory goes down.

Azure AD pass-through authentication. Azure AD pass-through authentication allows users to sign in to both on-premises and cloud-based applications using the same passwords, like password hash synch. A key difference, however, is when users sign in using Azure AD, pass-through authentication validates users' passwords directly against your on-premises Active Directory. Password validation doesn't happen in the cloud. This can be an important factor for organizations wanting to enforce their on-premises Active Directory security and password policies.

Azure AD pass-through authentication also uses Azure AD Connect but has the additional requirement of running one or more authentication agents. These agents serve as intermediary between Azure AD and the on-premises Active Directory in the process of authenticating users.

When a user tries to access an application to which they aren't already signed in, they get redirected to the Azure AD sign-in page to enter their username and password. Azure AD will encrypt the user password with the public key of the Authentication Agent. The on-premises Authentication Agent retrieves the username and encrypted password from Azure AD, decrypts the password with its private key, and validates the username and password against Active Directory. Active Directory evaluates the request and provides a response (success, failure, password expired, or user locked out) back to the agent, who then notifies Azure AD. If the response indicates success, then Azure AD will respond by authenticating the user.

The use of authentication agents running on a server, means a larger infrastructure footprint is required, when compared to password hash synchronization. Also, because pass-through authentication validates against the on-premises Active Directory with dependency on authentication agents running on servers, consideration should be given to distributed, redundant software and hardware to provide high availability of sign-in requests. Otherwise, if your datacenter suffers outage, authentication to Microsoft 365 services would no longer be possible.

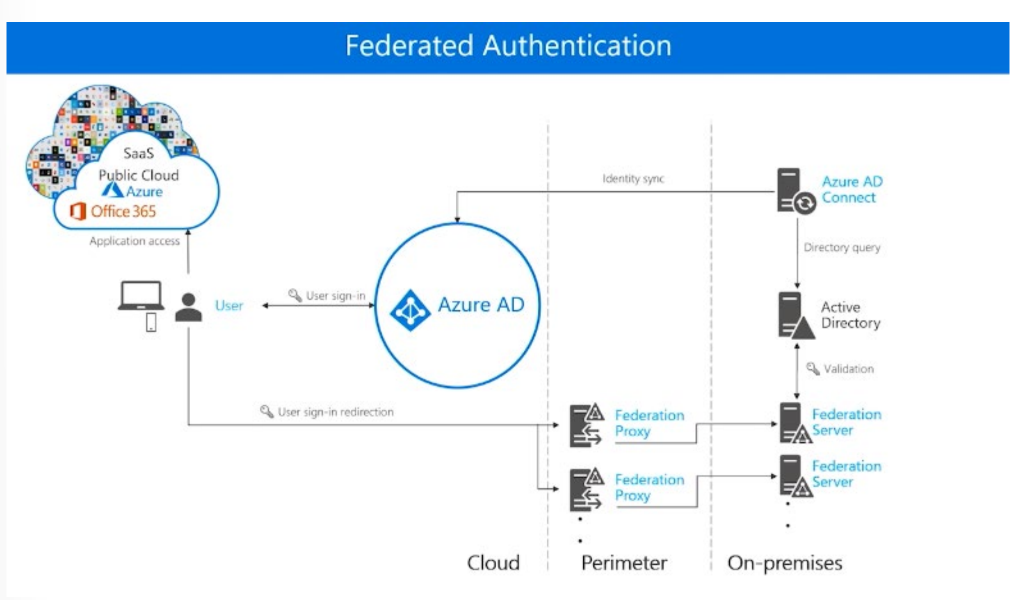


Federated authentication. Federation is recommended as an authentication for organizations that have advanced features not currently supported in Azure AD, including sign-on using smart cards or certificates, sign-on using on-premises multi-factor authentication (MFA) server, and sign-on using a third party authentication solution.

In federated authentication, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user's password. This sign-in method ensures that all user authentication occurs on-premises.

Federated authentication uses Azure AD Connect but also requires additional servers to support federation, resulting in a larger infrastructure footprint.

Organizations that decide to use Federation with Active Directory Federation Services (AD FS), can optionally set up password hash synchronization as a backup in case their AD FS infrastructure fails.



Knowledge check

Multiple choice

Item 1. Your organization is launching a new app for customers. You want your customers to use a sign-in screen that is customized with your brand identity. Which type of Azure External identity authentication solution should you use?

- ☐ Azure AD B2B
- ☐ Azure AD B2C
- ☐ Azure AD Hybrid identities

Multiple choice

Item 2. An organization has completed a full migration to the cloud and has purchased devices for all its employees. All employees sign in to the device through an organizational account configured in Azure AD. Select the option that best describes how these devices are set up in Azure AD.

- ☐ These devices are set up as Azure AD registered.
- ☐ These devices are set up as Azure AD joined.
- ☐ These devices are set up as Hybrid Azure AD joined.

Multiple choice

Item 3. A developer wants an application to connect to Azure resources that support Azure AD authentication, without having to manage any credentials and without incurring any extra cost. Which option best describes the identity type of the application?

- ☐ Service principal
- ☐ Managed identity
- ☐ Hybrid identity

Summary and resources

In this lesson, you've gained an insight into the features and capabilities of Azure Active Directory. You've learned about the different Azure AD editions, the identity types supported by Azure AD, and how you can use it to support external users. Finally, you learned about the hybrid model, where all user identities are managed in your on-premises Active Directory Domain Services (AD DS) directory, and changes are synchronized to your Azure AD.

Now that you've completed this lesson, you'll be able to:

- Describe what Azure AD does.
- Describe the identity types that Azure AD supports.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **What is Azure Active Directory?**[6]
- **Azure AD Licenses**[7]
- **Azure Active Directory External Identities**[8]
- **Azure Active Directory B2C documentation**[9]
- **Managed identities**[10]
- **Services that support managed identities for Azure resources**[11]
- **Azure AD registered devices**[12]
- **Azure AD joined devices**[13]
- **Hybrid Azure AD joined devices**[14]
- **Choose the right authentication method for your Azure Active Directory hybrid identity solution**[15]
- **What is Azure AD Connect?**[16]
- **Implement password hash synchronization with Azure AD Connect sync**[17]
- **User sign-in with Azure Active Directory Pass-through Authentication**[18]
- **What is federation with Azure AD?**[19]

6 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis
7 https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis#what-are-the-azure-ad-licenses
8 https://docs.microsoft.com/azure/active-directory/external-identities/compare-with-b2c
9 https://docs.microsoft.com/azure/active-directory-b2c/
10 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/overview
11 https://docs.microsoft.com/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities
12 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-register
13 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join
14 https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join-hybrid
15 https://docs.microsoft.com/azure/active-directory/hybrid/choose-ad-authn
16 https://docs.microsoft.com/azure/active-directory/hybrid/whatis-azure-ad-connect
17 https://docs.microsoft.com/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
18 https://docs.microsoft.com/azure/active-directory/hybrid/how-to-connect-pta
19 https://docs.microsoft.com/azure/active-directory/hybrid/whatis-fed

Describe the authentication capabilities of Azure AD

Introduction

Authentication is the process of verifying an identity to be legitimate. Passwords are commonly used to authenticate users, but there are better and more secure ways to authenticate.

In this lesson, you'll learn about the authentication capabilities of Azure AD, multi-factor authentication, and how it improves security. You'll also find out about the password protection and management capabilities of Azure AD.

After completing this lesson, you'll be able to:

- Describe the authentication methods of Azure AD.
- Describe multi-factor authentication in Azure AD
- Describe the password protection and management capabilities of Azure AD.

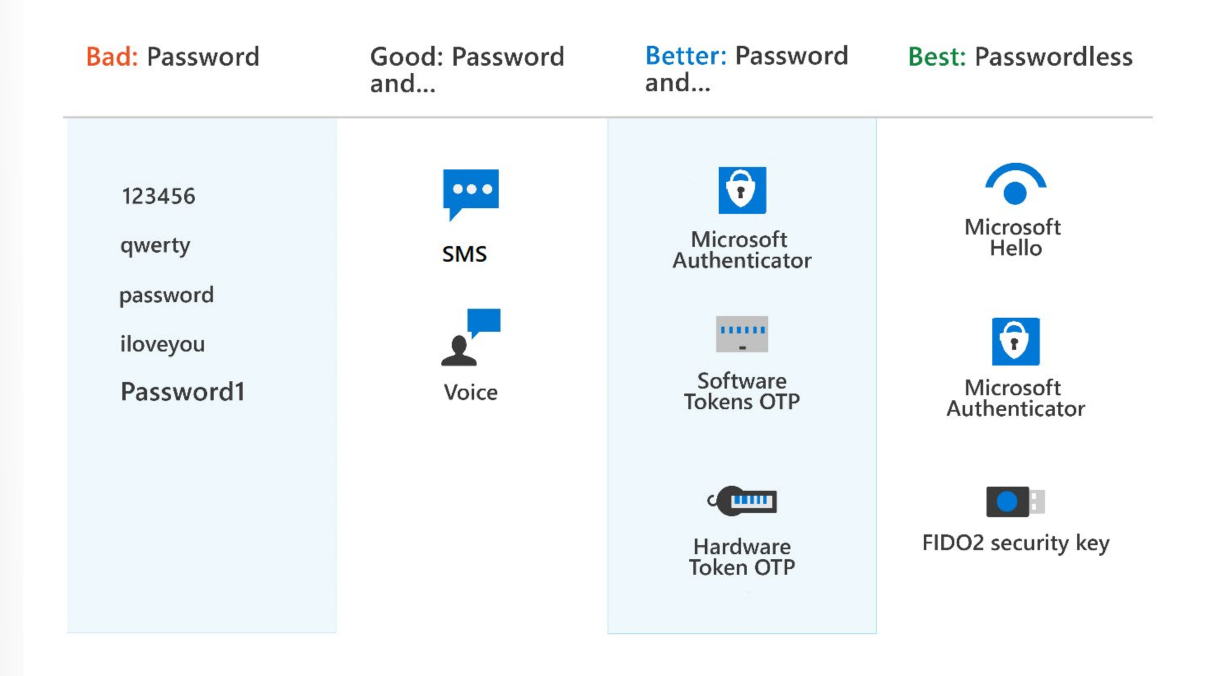
Describe the different authentication methods of Azure AD

One of the main features of an identity platform is to verify, or authenticate, credentials when a user signs in to a device, application, or service. Azure AD offers different methods of authentication.

Passwords

Passwords are the most common form of authentication, but they have many problems, especially if used in single-factor authentication, where only one form of authentication is used. If they're easy enough to remember, they're easy for a hacker to compromise. Strong passwords that aren't easily hacked are difficult to remember and affect user productivity when forgotten.

The use of passwords should be supplemented or replaced with more secure authentication methods available in Azure AD.



Phone

Azure AD supports two options for phone-based authentication.

- **SMS-based authentication**. Short message service (SMS) used in mobile device text messaging can be used as a primary form of authentication. With SMS-based sign in, users don't need to know a username and password to access applications and services. The user instead enters their registered mobile phone number, receives a text message with a verification code, and enters that in the sign-in interface.

  Users can also choose to verify their identity through SMS text messaging on a mobile phone, as a secondary form of authentication during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication. For example, users can supplement their password by using SMS text messaging. An SMS is sent to the mobile phone number containing a verification code. To complete the sign-in process, the verification code provided is entered into the sign-in interface.

- **Voice call verification**. Users can use voice calls as a secondary form of authentication, to verify their identity, during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication. With phone call verification, an automated voice call is made to the phone number registered by the user. To complete the sign-in process, the user is prompted to press # on their keypad. Voice calls are not supported as a primary form of authentication, in Azure AD.

OATH

OATH (Open Authentication) is an open standard that specifies how time-based, one-time password (TOTP) codes are generated. One-time password codes can be used to authenticate a user. OATH TOTP is implemented using either software or hardware to generate the codes.

- **Software OATH tokens** are typically applications. Azure AD generates the secret key, or seed, that's input into the app and used to generate each OTP.

- **OATH TOTP hardware tokens** (supported in public preview) are small hardware devices that look like a key fob that displays a code that refreshes every 30 or 60 seconds. OATH TOTP hardware tokens typically come with a secret key, or seed, pre-programmed in the token. These keys and other information specific to each token must be input into Azure AD and then activated for use by end-users.

OATH software and hardware tokens, are only supported as secondary forms of authentication in Azure AD, to verify an identity during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication.

Passwordless authentication

The end-goal for many organizations is to remove the use of passwords as part of sign-in events. When a user signs in with a passwordless method, credentials are provided by using methods like biometrics with Windows Hello for Business, or a FIDO2 security key. These authentication methods can't be easily duplicated by an attacker.

Azure AD provides ways to natively authenticate using passwordless methods to simplify the sign-in experience for users and reduce the risk of attacks.

To learn more about passwordless authentication, watch **The new sign-in standard: Passwordless authentication**[20].

Windows Hello for Business

Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This two-factor authentication is a combination of a key or certificate tied to a device and something that the person knows (a PIN) or something that the person is (biometrics). PIN entry and biometric gesture both trigger the use of the private key to cryptographically sign data that is sent to the identity provider. The identity provider verifies the user's identity and authenticates the user.

Windows Hello for Business helps protect against credential theft, because an attacker must have both the device and the biometric info or PIN, making it more difficult to gain access without the employee's knowledge.

As a passwordless authentication method, Windows Hello for Business serves as a primary form of authentication. In addition, Windows Hello for Business can be used as a secondary form of authentication to verify an identity during multi-factor authentication.

FIDO2

Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources using an external security key or a platform key built into a device, eliminating the need for a username and password.

FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard and is supported by Azure AD. FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. These FIDO2 security keys are typically USB devices, but could also be Bluetooth or Near Field Communication (NFC) based devices, which are used for short-range wireless data transfer. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.

With FIDO2 security keys, users can sign in to Azure AD or hybrid Azure AD joined Windows 10 devices and get single-sign on to their cloud and on-premises resources. Users can also sign in to supported

20 https://www.microsoft.com/en-us/videoplayer/embed/RE4zhD7

browsers. FIDO2 security keys are a great option for enterprises who are very security sensitive or have scenarios or employees who aren't willing or able to use their phone as a second factor.

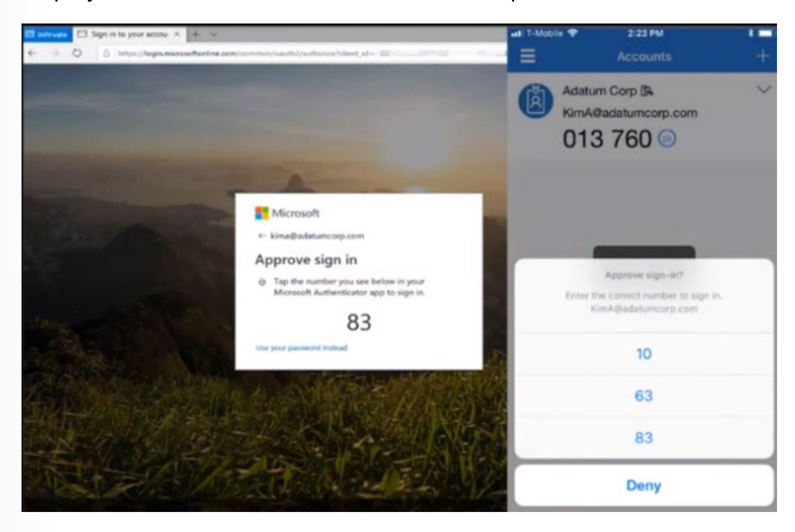
As a passwordless authentication method, FIDO2 serves as a primary form of authentication. In addition, FIDO2 can be used as a secondary form of authentication to verify an identity during multi-factor authentication.

Microsoft Authenticator app

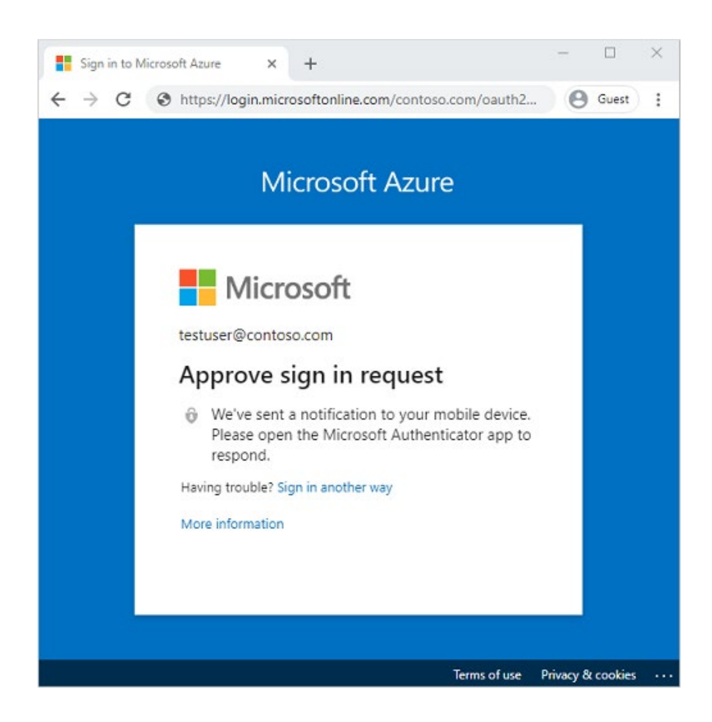
The Microsoft Authenticator app can be used as a passwordless authentication option, to sign into any Azure AD account or as an additional verification option during self-service password reset (SSPR) or Azure AD Multi-Factor Authentication events.

To use Microsoft Authenticator, a user must download the phone app from the Microsoft store and register their account. Microsoft Authenticator is available for Android and iOS.

With Passwordless sign in, the Authenticator App turns any iOS or Android phone into a strong, passwordless credential. To sign in to their Azure AD account, a user enters their username, matches a number displayed on the screen to the one on their phone, then uses their biometric or PIN to confirm.



When a user chooses Authenticator as secondary form of authentication, to verify their identity, a notification is pushed to the phone or tablet. If the notification is legitimate, the user selects **Approve**, otherwise, they select **Deny**.



Describe Multi-factor authentication in Azure AD

Multi-factor authentication requires more than one form of verification, such as a trusted device or a fingerprint scan, to prove that an identity is legitimate. It means that, even when an identity's password has been compromised, a hacker can't access a resource.

Multi-factor authentication dramatically improves the security of an identity, while still being simple for users. The extra authentication factor must be something that's difficult for an attacker to obtain or duplicate.

Azure Active Directory Multi-Factor Authentication works by requiring:

- **Something you know** – typically a password or PIN **and**
- **Something you have** – such as a trusted device that's not easily duplicated, like a phone or hardware key **or**
- **Something you are** – biometrics like a fingerprint or face scan.

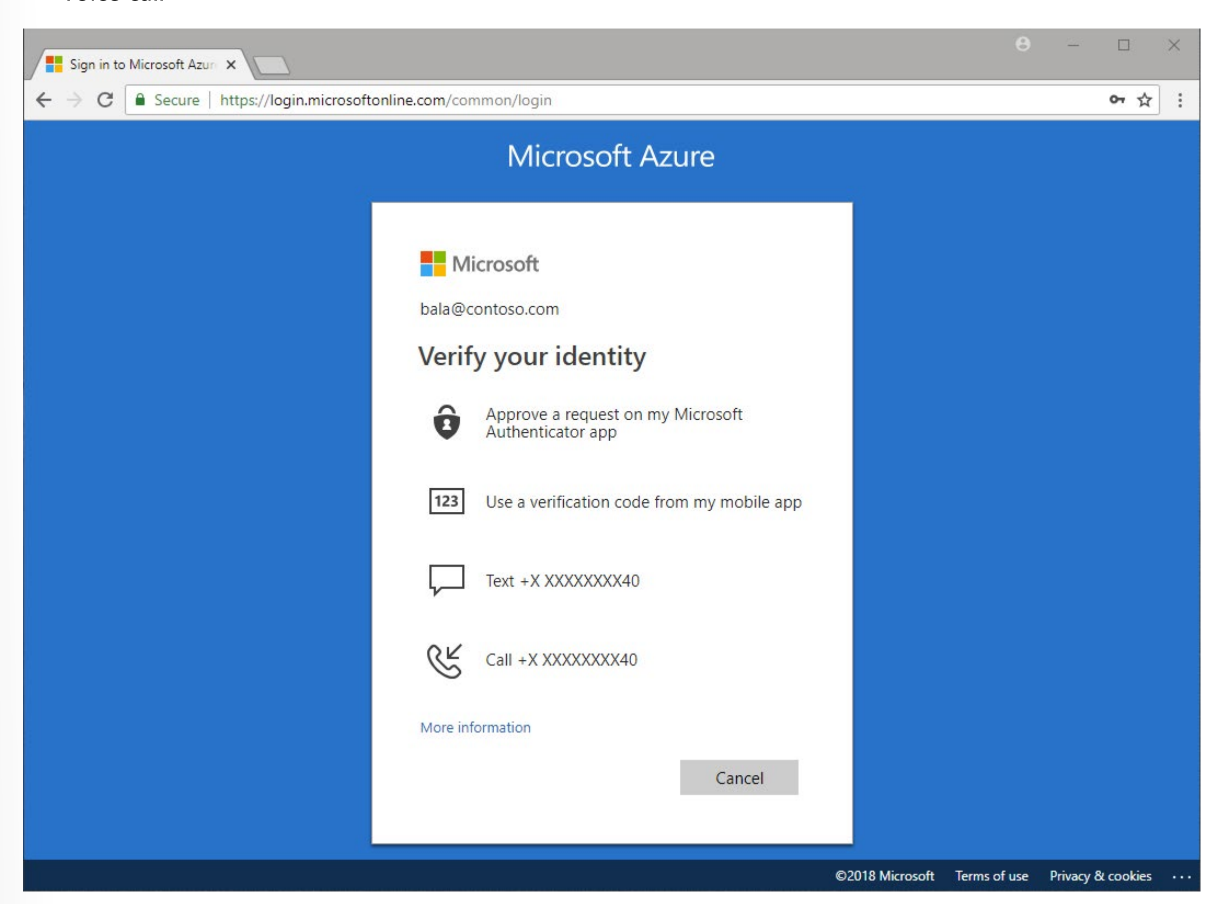
Multi-factor authentication verification prompts are configured to be part of the Azure AD sign-in event. Azure AD automatically requests and processes multi-factor authentication, without you making any changes to your applications or services. When a user signs in, they receive a multi-factor authentication prompt, and can choose from one of the additional verification forms that they've registered.

An administrator can require certain verification methods, or the user can access their MyAccount to edit or add verification methods.

The following additional forms of verification, described in the previous unit, can be used with Azure AD Multi-Factor Authentication:

- Microsoft Authenticator app
- Windows Hello for Business

- FIDO2 security key
- OATH hardware token (preview)
- OATH software token
- SMS
- Voice call



Security defaults and multi-factor authentication

Security defaults are a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. These defaults enable some of the most common security features and controls, including:

- Enforcing Azure Active Directory Multi-Factor Authentication registration for all users.
- Forcing administrators to use multi-factor authentication.
- Requiring all users to complete multi-factor authentication when needed.

Security defaults are a great option for organizations that want to increase their security posture but don’t know where to start, or for organizations using the free tier of Azure AD licensing. Security defaults may not be appropriate for organizations with Azure AD premium licenses or more complex security requirements. To learn more, visit **What are security defaults?**[21]

21 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Describe self-service password reset in Azure AD

Self-service password reset (SSPR) is a feature of Azure AD that allows users to change or reset their password, without administrator or help desk involvement.

If a user's account is locked or they forget the password, they can follow a prompt to reset it and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.

Self-service password reset works in the following scenarios:

- **Password change**: when a user knows their password but wants to change it to something new.
- **Password reset**: when a user can't sign in, such as when they forget the password, and want to reset it.
- **Account unlock**: when a user can't sign in because their account is locked out.

To use self-service password reset, users must be:

- Assigned an Azure AD license. Refer to the Learn More section of the summary and resources unit for a link to the Licensing requirements for Azure Active Directory self-service password reset.
- Enabled for SSPR by an administrator.
- Registered, with the authentication methods they want to use. Two or more authentication methods are recommended in case one is unavailable.

The following authentication methods are available for SSPR:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

When users register for SSPR, they're prompted to choose the authentication methods to use. If they choose to use security questions, they pick from a set of questions to prompt for and then provide their own answers. Security questions can only be used during the self-service password reset (SSPR) process to confirm who you are. Security questions aren't used as an authentication method during a sign-in event. Administrator accounts can't use security questions as verification method with SSPR.

IMPORTANT: By default, administrator accounts are enabled for self-service password reset and are required to use two authentication methods to reset their password, such as an email address, authenticator app, or a phone number. Administrators don't have the ability to use security questions.

When a user resets their password using self-service password reset, it can also be written back to an on-premises Active Directory. Password write-back allows users to use their updated credentials with on-premises devices and applications without a delay.

To keep users informed about account activity, admins can configure email notifications to be sent when an SSPR event happens. These notifications can cover both regular user accounts and admin accounts. For admin accounts, this notification provides an extra layer of awareness when a privileged administrator account password is reset using SSPR. All global admins would be notified when SSPR is used on an admin account.

In this interactive guide, you'll enable self-service password reset for users in Azure Active Directory. Select the link below to get started and follow the prompts on the screen.

Interactive guide - enable self-service password reset for users in Azure Active Directory.[22]

Describe password protection & management capabilities of Azure AD

Password Protection is a feature of Azure AD that reduces the risk of users setting weak passwords. Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block other weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list. When users change or reset their passwords, these lists are checked to enforce the use of strong passwords.

You should use extra features like Azure Active Directory Multi-Factor Authentication, not just rely on strong passwords enforced by Azure AD Password Protection.

Global banned password list

A global banned password list with known weak passwords is automatically updated and enforced by Microsoft. This list is maintained by the Azure AD Identity Protection team, who analyze security telemetry data to find weak or compromised passwords. Examples of passwords that might be blocked are P@$$w0rd or Passw0rd1 and all variations.

Variations are created using an algorithm that transposes text case and letters to numbers such as "1" to an "l". Variations on Password1 might include Passw0rd1, Pass0rd1, and others. These passwords are then checked and added to the global banned password list and made available to all Azure AD users. The global banned password list is automatically applied and can't be disabled.

If an Azure AD user tries to set their password to one of these weak passwords, they receive a notification to choose a more secure one. The global banned list is sourced from real-world, actual password spray attacks. This approach improves the overall security and effectiveness, and the password validation algorithm also uses smart fuzzy-matching techniques used to find strings that approximately match a pattern. Azure AD Password Protection efficiently detects and blocks millions of the most common weak passwords from being used in your enterprise.

Custom banned password lists

Admins can also create custom banned password lists to support specific business security needs. The custom banned password list prohibits passwords such as the organization name or location. Passwords added to the custom banned password list should be focused on organizational-specific terms such as:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms

22 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP02M03-Enable-SSPR-in-Azure-Active-Directory/index.html?azure-portal=true

- Abbreviations that have specific company meaning

The custom banned password list is combined with the global banned password list to block variations of all the passwords.

Banned password lists are a feature of Azure AD Premium 1 or 2.

Protecting against password spray

Azure AD Password Protection helps you defend against password spray attacks. Most password spray attacks submit only a few of the known weakest passwords against each of the accounts in an enterprise. This technique allows the attacker to quickly search for an easily compromised account and avoid potential detection thresholds.

Azure AD Password Protection efficiently blocks all known weak passwords likely to be used in password spray attacks. This protection is based on real-world security telemetry data from Azure AD, which is used to build the global banned password list.

Hybrid security

For hybrid security, admins can integrate Azure AD Password Protection within an on-premises Active Directory environment. A component installed in the on-premises environment receives the global banned password list and custom password protection policies from Azure AD. Domain controllers then use them to process password change events. This hybrid approach makes sure that, wherever a user changes their password, Azure AD Password Protection is applied.

Although password protection improves the strength of passwords, you should still use best practice features like Azure Active Directory Multi-Factor Authentication. Passwords alone, even strong ones, are not as secure as multiple layers of security.

Knowledge check

Multiple choice

Item 1. After hearing of a security breach at a competitor, you want to improve identity security within your organization. What should you implement immediately to provide the greatest protection to user identities?

☐ Multi-factor authentication.

☐ Require biometrics for all sign-in.

☐ Require strong passwords for all identities.

Multiple choice

Item 2. Which of the following additional forms of verification can be used with Azure AD Multi-Factor Authentication?

☐ Microsoft Authenticator app, SMS, Voice call, FIDO2, and Windows Hello for Business

☐ Security questions, SMS, Voice call, FIDO2, and Windows Hello for Business

☐ Password spray, SMS, Voice call, FIDO2, and Windows Hello for Business

Multiple choice

Item 3. A company's IT organization has been asked to find ways to reduce IT costs, without compromising security. Which feature should they consider implementing?

☐ Self-service password reset.

☐ Biometric sign-in on all devices.

☐ FIDO2.

Summary and resources

In this lesson, you've seen why passwords are a problematic form of authentication. You've learned about the different types of authentication that can be used with Azure AD, including passwordless authentication with Windows Hello for Business and the Microsoft Authenticator app. You've learned about multi-factor authentication.

You've learned how Azure AD can be configured to allow users to reset their own passwords, and how Azure AD Password Protection mitigates against the inherent risks associated with passwords.

Now that you've completed this lesson, you'll be able to:

- Describe the secure authentication methods of Azure AD.
- Describe Multi-factor authentication in Azure AD
- Describe the password protection and management capabilities of Azure AD.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **What is Azure Active Directory Authentication?**[23]
- **What authentication and verification methods are available in Azure Active Directory?**[24]
- **Authentication methods in Azure Active Directory - Microsoft Authenticator app**[25]
- **Authentication methods in Azure Active Directory - OATH tokens**[26]
- **Passwordless authentication options for Azure Active Directory**[27]
- **Authentication methods in Azure Active Directory - phone options**[28]
- **FIDO2 security keys**[29]
- **Windows Hello for Business**[30]
- **How it works: Azure AD Multi-Factor Authentication**[31]
- **What are security defaults?**[32]

23 https://docs.microsoft.com/azure/active-directory/authentication/overview-authentication
24 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-methods
25 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-authenticator-app
26 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-oath-tokens
27 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless
28 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-phone-options
29 https://docs.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
30 https://docs.microsoft.com/windows/security/identity-protection/hello-for-business/hello-overview
31 https://docs.microsoft.com/azure/active-directory/authentication/concept-mfa-howitworks
32 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

- **Enable users to unlock their account or reset passwords using Azure Active Directory self-service password reset**[33]
- **Eliminate bad passwords using Azure Active Directory Password Protection**[34]

33 https://docs.microsoft.com/azure/active-directory/authentication/tutorial-enable-sspr
34 https://docs.microsoft.com/azure/active-directory/authentication/concept-password-ban-bad

Describe the access management capabilities of Azure AD

Introduction

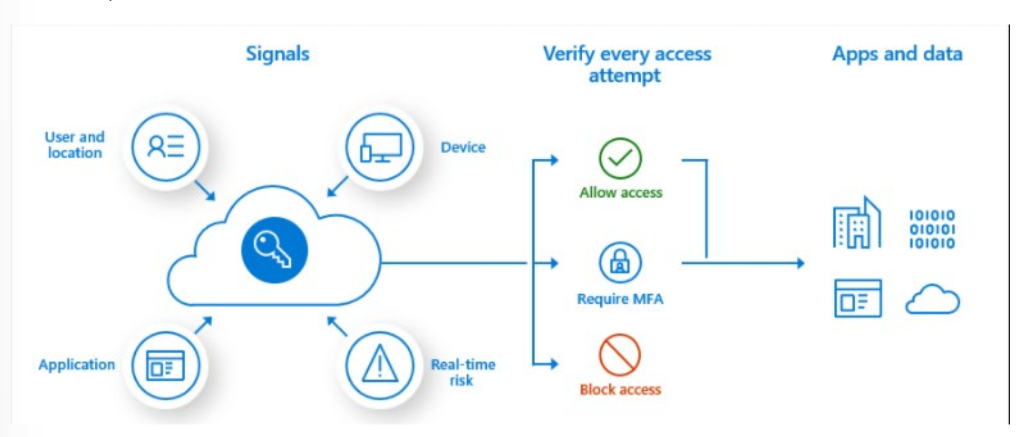
One of the main purposes of Azure AD is to manage access. The security perimeter has shifted away from organizational boundaries to user, device, and service identities. In this lesson, you'll learn how Azure AD uses intelligent access management capabilities to protect organizational assets. This module describes how Conditional Access helps organization improve security. It also describes the benefits of Azure AD roles, role-based access control, and how they're used to control access to Azure AD resources.

In this lesson, you'll learn how to:

- Describe Conditional Access in Azure AD.
- Describe the benefits of Azure AD roles and role-based access control.

Describe conditional access in Azure AD

Conditional Access is a feature of Azure AD that provides an additional layer of security before allowing authenticated users to access data or other assets. Conditional Access is implemented through policies that are created and managed in Azure AD. A Conditional Access policy analyses signals including user, location, device, application, and risk to automate decisions for authorizing access to resources (apps and data).



A conditional access policy might state that IF a user belongs to a certain group, then they're required to provide multi-factor authentication to sign in to an application.

Watch this video, **Conditional Access**[35], to see how Conditional Access policies work.

Conditional Access signals

Some of the common signals that Conditional Access can take in to account when making a policy decision may include:

- **User or group membership**. Policies can be targeted to all users, specific groups of users, directory roles, or external guest users, giving administrators fine-grained control over access.

35 https://www.microsoft.com/videoplayer/embed/RE4INyI

- **Named location information**. Named location information can be created using IP address ranges, and used when making policy decisions. Also, administrators can opt to block or allow traffic from an entire country/region's IP range.
- **Device**. Users with devices of specific platforms or marked with a specific state can be used.
- **Application**. Users attempting to access specific applications can trigger different Conditional Access policies.
- **Real-time sign in risk detection**. Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior - the probability that a given sign-in, or authentication request, isn't authorized by the identity owner. Policies can then force users to perform password changes or multi factor authentication to reduce their risk level or be blocked from access until an administrator takes manual action.
- **Cloud apps or actions**. Cloud apps or actions can include or exclude cloud applications or user actions that will be subject to the policy.
- **User risk**. For customers with access to Identity Protection, user risk can be evaluated as part of a Conditional Access policy. User risk represents the probability that a given identity or account is compromised. User risk can be configured for high, medium, or low probability.

When creating a conditional access policy, admins can determine which signals to use through assignments. The assignments portion of the policy controls the who, what, and where of the Conditional Access policy. All assignments are logically ANDed. If you have more than one assignment configured, all assignments must be satisfied to trigger a policy.

Access controls

When the Conditional Access policy has been applied, an informed decision is reached on whether to grant access, block access, or require extra verification. The decision is referred to as the access controls portion of the Conditional Access policy and defines how a policy is enforced. Common decisions are:

- Block access
- Grant access
- Require one or more conditions to be met before granting access:
  - Require multi-factor authentication.
  - Require device to be marked as compliant.
  - Require hybrid Azure AD joined device.
  - Require approved client app.
  - Require app protection policy.
  - Require password change.
- Control user access based on session controls to enable limited experiences within specific cloud applications. As an example, Conditional Access App Control uses signals from Microsoft Defender for Cloud Apps to block the download, cut, copy, and print capabilities for sensitive documents, or to require labeling of sensitive files. Other session controls include sign in frequency and application enforced restrictions that, for selected applications, use the device information to provide users with a limited or full experience, depending on the device state.

Conditional Access policies can be targeted to members of specific groups or guests. For example, you can create a policy to exclude all guest accounts from accessing sensitive resources.
Conditional Access is a feature of paid Azure AD editions.

Interactive Guide

In this interactive guide, you'll create a conditional access policy for a group of users. Select the link below to get started and follow the prompts on the screen.

Interactive guide - create a conditional access policy for a group of users.[36]

Describe Azure AD roles and role-based access control

Azure AD roles control permissions to manage Azure AD resources. For example, allowing user accounts to be created, or billing information to be viewed. Azure AD supports built-in and custom roles.

Managing access using roles is known as **role-based access control (RBAC)**. Azure AD built-in and custom roles are a form of RBAC in that Azure AD roles control access to Azure AD resources. This is referred to as Azure AD RBAC.

Built-in roles

There are many Azure AD built-in roles, which are roles with a fixed set of permissions. A few of the most common built-in roles are:

- *Global administrator*: users with this role have access to all administrative features in Azure Active Directory. The person who signs up for the Azure Active Directory tenant automatically becomes a global administrator.
- *User administrator*: users with this role can create and manage all aspects of users and groups. This role also includes the ability to manage support tickets and monitor service health.
- *Billing administrator*: users with this role make purchases, manage subscriptions and support tickets, and monitor service health.

All built-in roles are preconfigured bundles of permissions designed for specific tasks. The fixed set of permissions included in the built-in roles can't be modified.

Custom roles

Although there are many built-in admin roles in Azure AD, custom roles give flexibility when granting access. A custom role definition is a collection of permissions that you choose from a preset list. The list of permissions to choose from are the same permissions used by the built-in roles. The difference is that you get to choose which permissions you want to include in a custom role.

Granting permission using custom Azure AD roles is a two-step process. The first step involves creating a custom role definition, consisting of a collection of permissions that you add from a preset list. Once you've created your custom role definition, the second step is to assign that role to users or groups by creating a role assignment.

A role assignment grants the user the permissions in a role definition, at a specified scope. A scope defines the set of Azure AD resources the role member has access to. A custom role can be assigned at organization-wide scope, meaning the role member has the role permissions over all resources. A custom role can also be assigned at an object scope. An example of an object scope would be a single applica-

36 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP02M04-Create-a-Conditional-Access-Policy/index.html?azure-portal=true

tion. The same role can be assigned to one user over all applications in the organization and then to another user with a scope of only the Contoso Expense Reports app.

Custom roles require an Azure AD Premium P1 or P2 license.

Only grant the access users need

It's best practice, and more secure, to grant users the least privilege to get their work done. It means that if someone mostly manages users, you should assign the user administrator role, and not global administrator. By assigning least privileges, you limit the damage that could be done with a compromised account.

Categories of Azure AD roles

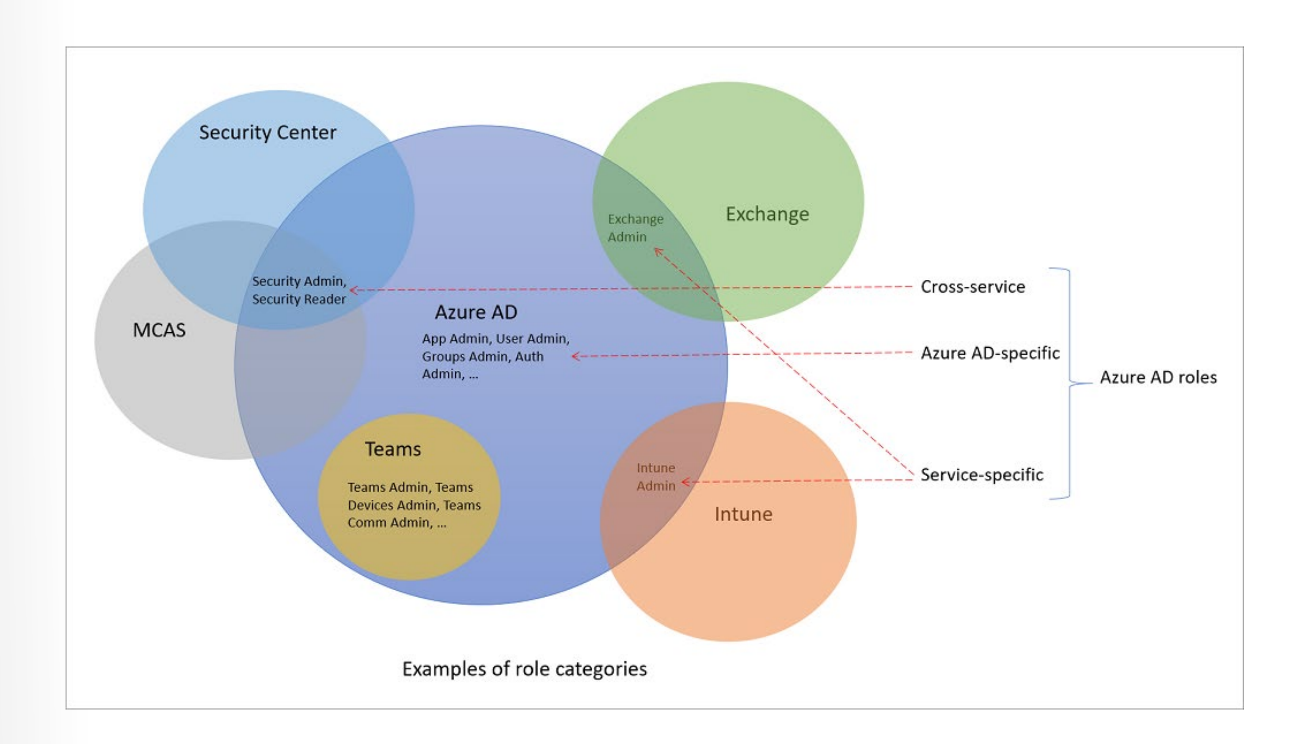
As previously defined, Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity and access management service. Azure AD is an available service, if you subscribe to any Microsoft Online business offer, such as Microsoft 365 and Azure.

Available Microsoft 365 services include Azure AD, Exchange, SharePoint, Microsoft Defender, Teams, Intune, and many more.

Over time, some Microsoft 365 services, such as Exchange and Intune, have developed their own role-based access control systems, just like the Azure AD service has Azure AD roles to control access to Azure AD resources (Azure AD RBAC). Other services such as Teams and SharePoint don’t have separate role-based access control systems, they use Azure AD roles for their administrative access.

To make it convenient to manage identity across Microsoft 365 services, Azure AD has added some service-specific, built-in roles, each of which grants administrative access to a Microsoft 365 service. This means that Azure AD built-in roles differ in where they can be used. There are three broad categories.

- Azure AD-specific roles: These roles grant permissions to manage resources within Azure AD only. For example, User Administrator, Application Administrator, Groups Administrator all grant permissions to manage resources that live in Azure AD.
- Service-specific roles: For major Microsoft 365 services, Azure AD includes built-in, service-specific roles that grant permissions to manage features within the service. For example, Azure AD includes built-in roles for Exchange Administrator, Intune Administrator, SharePoint Administrator, and Teams Administrator roles that can manage features with their respective services.
- Cross-service roles: There are some roles within Azure AD that span services. For example, Azure AD has security-related roles, like Security Administrator, that grant access across multiple security services within Microsoft 365. Similarly the Compliance Administrator role you can manage Compliance-related settings in Microsoft Purview compliance portal, Exchange, and so on.

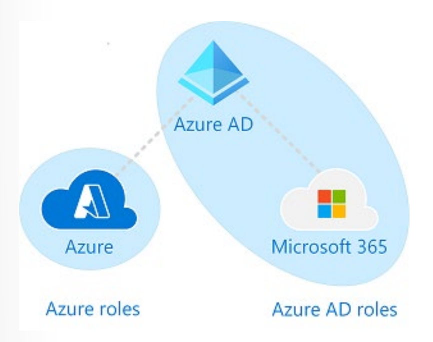


Difference between Azure AD RBAC and Azure RBAC

As described above, Azure AD built-in and custom roles are a form of RBAC in that Azure AD roles control access to Azure AD resources. This is referred to as Azure AD RBAC. In the same way that Azure AD roles can control access to Azure AD resources, so too can Azure roles control access to Azure resources. This is referred to as Azure RBAC. Although the concept of RBAC applies to both Azure AD RBAC and Azure RBAC, what they control are different.

- Azure AD RBAC - Azure AD roles control access to Azure AD resources such as users, groups, and applications.
- Azure RBAC - Azure roles control access to Azure resources such as virtual machines or storage using Azure Resource Management.

There are different data stores where role definitions and role assignments are stored. Similarly, there are different policy decision points where access checks happen.



Knowledge check

Multiple choice

Item 1. You've been asked to implement conditional access for your organization, what must you do?

- ☐ Create and assign a policy that enforces organizational rules.
- ☐ Check that all users have multi-factor authentication enabled.
- ☐ Amend your apps to allow conditional access.

Multiple choice

Item 2. Sign-in risk is a signal used by conditional access policies to decide whether to grant or deny access. What is sign in risk?

- ☐ The probability that the device is owned by the identity owner.
- ☐ The probability that the authentication request isn't authorized by the identity owner.
- ☐ The probability that the user is authorized to view data from a particular application.

Multiple choice

Item 3. You've been asked to review Azure AD roles assigned to users to improve organizational security. Which of the following should you implement?

- ☐ Remove all Global Admin roles assigned to users.
- ☐ Create custom roles.
- ☐ Replace Global Admin roles with specific Azure AD roles.

Summary and resources

In this lesson, you've learned about Conditional Access and how it's used to protect resources. You've seen how Conditional Access policies use *if then* statements with signals to determine whether to grant access, require more information, or block access.

You also learned about built-in and custom roles in Azure AD and how these are used to provide role-based access control in Azure AD

Now that you've completed this lesson, you'll be able to:

- Describe Conditional Access in Azure AD.
- Describe the benefits of Azure AD roles and role-based access control.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Conditional Access**[37]
- **Security defaults**[38]

37 https://docs.microsoft.com/azure/active-directory/conditional-access/overview
38 https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

- **Available roles**[39]
- **Custom administrator roles in Azure AD**[40]
- **Understand Azure Active Directory role concepts**[41]

39 https://docs.microsoft.com/azure/active-directory/roles/permissions-reference
40 https://docs.microsoft.com/azure/active-directory/roles/custom-overview
41 https://docs.microsoft.com/azure/active-directory/roles/concept-understand-roles

Describe the identity protection and governance capabilities of Azure AD

Introduction

Identity governance is about balancing identity security with user productivity in a way that can be justified and audited. Azure AD provides many identity protection and governance capabilities, including Privileged Identity Management (PIM), Identity Protection, and terms of use statements.

In this lesson, you'll learn how to:

- Describe the identity governance capabilities of Azure AD.
- Describe Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

Describe identity governance in Azure AD

Azure AD identity governance gives organizations the ability to do the following tasks:

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

These actions can be completed for employees, business partners and vendors, and across services and applications, both on-premises and in the cloud.

It's intended to help organizations address these four key questions:

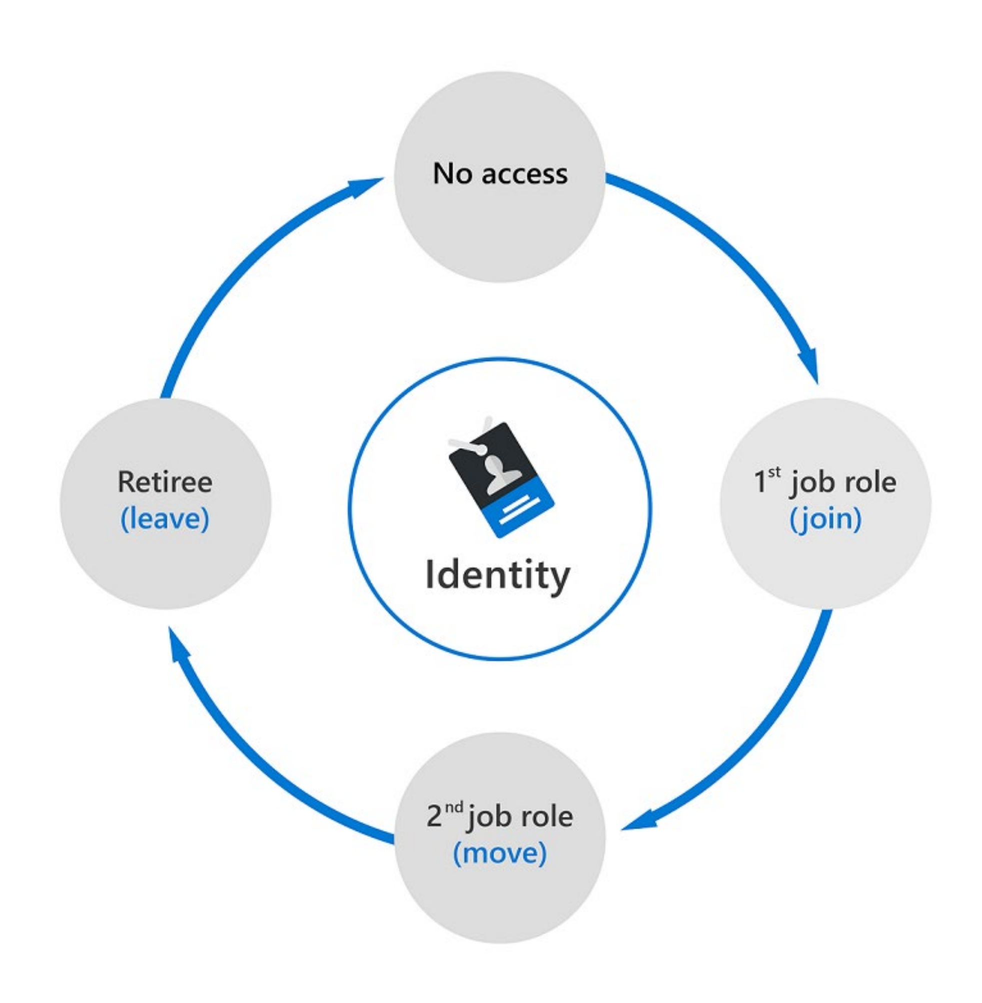
- Which users should have access to which resources?
- What are those users doing with that access?
- Are there effective organizational controls for managing access?
- Can auditors verify that the controls are working?

Identity lifecycle

Managing users' identity lifecycle is at the heart of identity governance.

When planning identity lifecycle management for employees, for example, many organizations model the "join, move, and leave" process. When an individual first joins an organization, a new digital identity is created if one isn't already available. When an individual moves between organizational boundaries, more access authorizations may need to be added or removed to their digital identity. When an individual leaves, access may need to be removed, and the identity might no longer be required, other than for audit purposes.

The diagram below shows a simplified version of the identity lifecycle.



For many organizations, this identity lifecycle for employees is tied to the representation of that user in a human resources (HR) system such as Workday or SuccessFactors. The HR system is authoritative for providing the current list of employees, and some of their properties, such as name or department.

Azure AD Premium offers integration with cloud-based HR systems. When a new employee is added to an HR system, Azure AD can create a corresponding user account. Similarly, when their properties, such as department or employment status, change in the HR system, synchronization of those updates to Azure AD ensures consistency.

Azure AD Premium also includes Microsoft Identity Manager, which can import records from on-premises HR systems such as SAP HCM, Oracle eBusiness, and Oracle PeopleSoft. For more information, refer to the Microsoft Identity Manager documentation that is listed in the Learn More section of the Summary and resources unit.

In general, managing the lifecycle of an identity is about updating the access that users need, whether through integration with an HR system, or through the user provisioning applications.

Access lifecycle

Access lifecycle is the process of managing access throughout the user's organizational life. Users require different levels of access from the point at which they join an organization to when they leave it. At

various stages in between, they'll need access rights to different resources depending on their role and responsibilities.

Organizations can automate the access lifecycle process through technologies such as dynamic groups. Dynamic groups enable admins to create attribute-based rules to determine membership of groups. When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any users to be added or removed from a group. If a user or device satisfies a rule for a group, they're added as a member of that group. If they no longer satisfy the rule, they're removed.

Privileged access lifecycle

Monitoring privileged access is a key part of identity governance. When employees, vendors, and contractors are assigned administrative rights, there should be a governance process because of the potential for misuse.

Azure AD Privileged Identity Management (PIM) provides extra controls tailored to securing access rights. PIM helps you minimize the number of people who have access to resources across Azure AD, Azure, and other Microsoft online services. PIM provides a comprehensive set of governance controls to help secure your company's resources. PIM is a feature of Azure AD Premium P2.

Describe entitlement management, access reviews, and terms of use

Entitlement management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale. Entitlement management automates access request workflows, access assignments, reviews, and expiration.

Enterprise organizations often face challenges when managing employee access to resources such as:

- Users may not know what access they should have, and even if they do, they might have difficulty locating the right individuals to approve it.
- When users find and receive access to a resource, they may hold on to access longer than is required for business purposes.
- Managing access for external users.

Entitlement management includes the following capabilities to address these challenges:

- Delegate the creation of access packages to non-administrators. These access packages contain resources that users can request. The delegated access package managers then define policies that include rules such as which users can request access, who must approve their access, and when access expires.
- Managing external users. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

The video, **What is Azure AD entitlement management?**[42] introduces entitlement management, and looks at how access packages are used to give access to resources.

Entitlement management is a feature of Azure AD Premium P2.

42 https://www.microsoft.com/videoplayer/embed/RE4JXQr

Azure AD access reviews

Azure Active Directory (AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment. Regular access reviews ensure that only the right people have access to resources. Excessive access rights are a known security risk. However, when people move between teams, or take on or relinquish responsibilities, access rights can be difficult to control.

Access reviews are helpful when:

- You have too many users in privileged roles, such as global administrator.
- When automation isn't possible, such as when HR data isn't in Azure AD.
- You want to control business critical data access.
- Your governance policies require periodic reviews of access permissions.

Access reviews can be created through Azure AD access reviews, or Azure AD Privileged Identity Management (PIM). Access reviews can be used to review and manage access for both users and guests. When an access review is created, it can be set up so that each user reviews their own access, or to have one or more users review everyone's access. Similarly, all guests can be asked to review their own access, or have it looked at by one or more users.

Admins who create access reviews can track progress as the reviewers complete their process. No access rights are changed until the review is finished. You can, however, stop a review before it reaches its scheduled end.

When the review is complete, it can be set to manually or auto-apply changes to remove access from a group membership or application assignment, except for a dynamic group or a group that originates on-premises. In those cases, the changes must be applied directly to the group.

Access reviews are a feature of Azure AD Premium P2.

Azure AD terms of use

Azure AD terms of use allow information to be presented to users, before they access data or an application. Terms of use ensure users read relevant disclaimers for legal or compliance requirements.

Employees or guests can be required to accept terms of use in the following situations:

- Before they access sensitive data or an application.
- On a recurring schedule, so they're reminded of regulations.
- When terms of use are required in different languages.
- Based on user attributes, such as terms applicable to certain roles.
- Presenting terms for all users in your organization.

Terms of use are presented in a PDF format, using content that you create, such as an existing contract document. Terms of use can also be presented to users on mobile devices.

Conditional Access policies are used to require a terms of use statement being displayed, and ensuring the user has agreed to those terms before accessing an application. Admins can then view who has agreed to terms of use, and who has declined.

Describe the capabilities of Privileged identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These include resources in Azure AD, Azure, and other Microsoft online services such as Microsoft 365 or Microsoft Intune. PIM mitigates the risks of excessive, unnecessary, or misused access permissions. It requires justification to understand why users want permissions, and enforces multi-factor authentication to activate any role.

PIM is:

- Just in time, providing privileged access only when needed, and not before.
- Time-bound, by assigning start and end dates that indicate when a user can access resources.
- Approval-based, requiring specific approval to activate privileges.
- Visible, sending notifications when privileged roles are activated.
- Auditable, allowing a full access history to be downloaded.

Privileged Identity Management is a feature of Azure AD Premium P2.

Why use PIM?

PIM reduces the chance of a malicious actor getting access by minimizing the number of people who have access to secure information or resources. By time-limiting authorized users, it reduces the risk of an authorized user inadvertently affecting sensitive resources. PIM also provides oversight for what users are doing with their administrator privileges. PIM mitigates the risk to organizations of elevated privileges.

For a more detailed look at PIM and why you might use it, watch **What is Privileged Identity Management?**[43].

Describe Azure Identity Protection

Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Microsoft analyses 6.5 trillion signals per day to identify potential threats. These signals come from learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox.

The signals generated by these services are fed to Identity Protection. These signals can then be used by tools such as Conditional Access, which uses them to make access decisions. Signals are also fed to security information and event management (SIEM) tools, such as Microsoft Sentinel, for further investigation.

Identity Protection categorizes risk into three tiers: low, medium, and high. It can also calculate the sign-in risk, and user identity risk.

A sign in risk represents the probability that a given authentication request isn't authorized by the identity owner. Sign in risk can be calculated in real-time or calculated offline using Microsoft's internal and external threat intelligence sources. Listed below are some of the sign-in risks that Identity Protection in Azure AD is able to identify:

- Anonymous IP address. This risk detection type indicates a sign-in from an anonymous IP address; for example, a Tor browser or anonymized VPNs.
- Atypical travel. This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior.
- Malware linked IP address. This risk detection type indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server.
- Unfamiliar sign in properties. This risk detection type considers past sign-in history to look for anomalous sign-ins. The system stores information about previous locations used by a user, and considers these “familiar” locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations.
- Password spray. This risk detection is triggered when a password spray attack has been performed.
- Azure AD threat intelligence. This risk detection type indicates sign in activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

43 https://www.microsoft.com/videoplayer/embed/RE4JXQr

A user risk represents the probability that a given identity or account is compromised. These risks are calculated offline using Microsoft's internal and external threat intelligence sources. Listed below are some of the user risks that Identity Protection in Azure AD is able to identify:

- Leaked credentials. This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Azure AD users' current valid credentials to find valid matches.
- Azure AD threat intelligence. This risk detection type indicates user activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

Identity Protection only generates risk detections when correct credentials are used in the authentication request. If a user uses incorrect credentials, it will not be flagged by Identity Protection since there isn't a risk of credential compromise unless a bad actor uses the correct credentials.
Risk detections can then trigger actions such as requiring users to provide multi-factor authentication, reset their password, or block access until an administrator takes action.

Identity Protection provides organizations with three reports that they can use to investigate identity risks in their environment. These reports are the **risky users**, **risky sign-ins**, and **risk detections**. Investigation of events is key to understanding and identifying any weak points in your security strategy.

After completing an investigation, admins will want to take action to remediate the risk or unblock users. Organizations can also enable automated remediation using their risk policies. Microsoft recommends closing events quickly because time matters when working with risk.

Identity Protection is a feature of Azure AD Premium P2.

Knowledge check

Multiple choice

Item 1. Your organization has implemented important changes in their customer facing web-based applications. You want to ensure that any user who wishes to access these applications agrees to the legal disclaimers. Which Azure AD feature should you implement?

☐ Identity protection.

☐ Entitlement management.

☐ Azure AD Terms of Use.

Multiple choice

Item 2. Your organization is project-oriented with employees often working on more than one project at a time. Which solution is best suited to managing user access to your organization's resources?

☐ Azure Terms of Use.

☐ Identity protection.

☐ Entitlement management.

Multiple choice

Item 3. Your organization has recently conducted a security audit and found that four people who have left the organization were still active and assigned Global Admin roles. The users have now been deleted and you've been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should you recommend?

- ☐ Entitlement Management.
- ☐ Privileged Identity Management.
- ☐ Identity protection.

Multiple choice

Item 4. You've recently discovered that several user accounts in the Finance Department have been compromised. Your CTO has asked for your help in finding a solution to reduce the impact of compromised user accounts. They've asked you to look at three Azure AD features, which one should you recommend?

- ☐ Identity protection.
- ☐ Conditional access.
- ☐ Entitlement management.

Summary and resources

In this lesson, you learned how Azure AD provides tools to help you govern the identity lifecycle and the access lifecycle. You also learned that Azure AD can be synchronized with human resources (HR) systems to manage identity lifecycles at scale.

This lesson discussed entitlement management, which automates access requests, access assignments, reviews, and expiration. You learned how these reviews can help you monitor who has access to what resources.

Finally, you learned how Privileged Identity Management (PIM) can help you minimize the number of users who have access to important resources, and how Identity Protection can detect potential identity risks.

Now that you've completed this lesson, you'll be able to:

- Describe the identity governance capabilities of Azure AD.
- Describe Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Azure AD Identity governance**[44]
- **Azure AD Privileged Identity Management**[45]
- **Azure AD access reviews**[46]

44 https://docs.microsoft.com/azure/active-directory/governance/identity-governance-overview
45 https://docs.microsoft.com/azure/active-directory/privileged-identity-management/pim-configure
46 https://docs.microsoft.com/azure/active-directory/governance/access-reviews-overview

- **Azure terms of use statements**[47]
- **Dynamic groups in Azure AD**[48]
- **Azure entitlement management**[49]
- **Azure Identity Protection**[50]
- **Microsoft Identity Manager**[51]

47 https://docs.microsoft.com/azure/active-directory/conditional-access/terms-of-use
48 https://docs.microsoft.com/azure/active-directory/enterprise-users/groups-dynamic-membership
49 https://docs.microsoft.com/azure/active-directory/governance/entitlement-management-overview
50 https://docs.microsoft.com/azure/active-directory/identity-protection/overview-identity-protection
51 https://docs.microsoft.com/microsoft-identity-manager/microsoft-identity-manager-2016

Answers

Multiple choice

Item 1. Your organization is launching a new app for customers. You want your customers to use a sign-in screen that is customized with your brand identity. Which type of Azure External identity authentication solution should you use?

☐ Azure AD B2B

■ Azure AD B2C

☐ Azure AD Hybrid identities

Explanation
Azure AD B2C is an authentication solution for customers that you can customize with your brand identity.

Multiple choice

Item 2. An organization has completed a full migration to the cloud and has purchased devices for all its employees. All employees sign in to the device through an organizational account configured in Azure AD. Select the option that best describes how these devices are set up in Azure AD.

☐ These devices are set up as Azure AD registered.

■ These devices are set up as Azure AD joined.

☐ These devices are set up as Hybrid Azure AD joined.

Explanation
An Azure AD joined device is a device joined to Azure AD through an organizational account, which is then used to sign in to the device. Azure AD joined devices are generally owned by the organization.

Multiple choice

Item 3. A developer wants an application to connect to Azure resources that support Azure AD authentication, without having to manage any credentials and without incurring any extra cost. Which option best describes the identity type of the application?

☐ Service principal

■ Managed identity

☐ Hybrid identity

Explanation
Managed identities are a type of service principal that are automatically managed in Azure AD and eliminate the need for developers to manage credentials.

Multiple choice

Item 1. After hearing of a security breach at a competitor, you want to improve identity security within your organization. What should you implement immediately to provide the greatest protection to user identities?

■ Multi-factor authentication.

☐ Require biometrics for all sign-in.

☐ Require strong passwords for all identities.

Explanation
Multi-factor authentication dramatically improves the security of an identity.

Multiple choice

Item 2. Which of the following additional forms of verification can be used with Azure AD Multi-Factor Authentication?

■ Microsoft Authenticator app, SMS, Voice call, FIDO2, and Windows Hello for Business

□ Security questions, SMS, Voice call, FIDO2, and Windows Hello for Business

□ Password spray, SMS, Voice call, FIDO2, and Windows Hello for Business

Explanation
Microsoft Authenticator app, SMS, Voice call, FIDO2, and Windows Hello for Business are all valid forms of verification with multi-factor authentication.

Multiple choice

Item 3. A company's IT organization has been asked to find ways to reduce IT costs, without compromising security. Which feature should they consider implementing?

■ Self-service password reset.

□ Biometric sign-in on all devices.

□ FIDO2.

Explanation
Self-service password reset allows users to change or reset their own passwords, thereby reducing the cost of providing administrators and help desk personnel.

Multiple choice

Item 1. You've been asked to implement conditional access for your organization, what must you do?

■ Create and assign a policy that enforces organizational rules.

□ Check that all users have multi-factor authentication enabled.

□ Amend your apps to allow conditional access.

Explanation
Conditional access is implemented using policies that enforce organizational rules.

Multiple choice

Item 2. Sign-in risk is a signal used by conditional access policies to decide whether to grant or deny access. What is sign in risk?

□ The probability that the device is owned by the identity owner.

■ The probability that the authentication request isn't authorized by the identity owner.

□ The probability that the user is authorized to view data from a particular application.

Explanation
Sign-in risk is the real-time calculation that a given authentication request isn't authorized by the identity owner.

Multiple choice

Item 3. You've been asked to review Azure AD roles assigned to users to improve organizational security. Which of the following should you implement?

☐ Remove all Global Admin roles assigned to users.

☐ Create custom roles.

■ Replace Global Admin roles with specific Azure AD roles.

Explanation
By following the least privilege security model and assigning specific admin roles such as billing administrator, or user administrator to more users, instead of global admin roles, you can improve organizational security.

Multiple choice

Item 1. Your organization has implemented important changes in their customer facing web-based applications. You want to ensure that any user who wishes to access these applications agrees to the legal disclaimers. Which Azure AD feature should you implement?

☐ Identity protection.

☐ Entitlement management.

■ Azure AD Terms of Use.

Explanation
Azure AD terms of use allow information to be presented to users, before they access data or an application, and can be configured to require users to accept the terms of use.

Multiple choice

Item 2. Your organization is project-oriented with employees often working on more than one project at a time. Which solution is best suited to managing user access to your organization's resources?

☐ Azure Terms of Use.

☐ Identity protection.

■ Entitlement management.

Explanation
Entitlement management is well suited to handling project-based access needs. Entitlement management automates access requests, access assignments, reviews, and expiration for bundles of resources relevant to a project.

Multiple choice

Item 3. Your organization has recently conducted a security audit and found that four people who have left the organization were still active and assigned Global Admin roles. The users have now been deleted and you've been asked to recommend a solution to prevent a similar security lapse happening in future. Which solution should you recommend?

☐ Entitlement Management.

■ Privileged Identity Management.

☐ Identity protection.

Explanation
Privileged Identity Management mitigates the risks of excessive, unnecessary, or misused access permissions.

Multiple choice

Item 4. You've recently discovered that several user accounts in the Finance Department have been compromised. Your CTO has asked for your help in finding a solution to reduce the impact of compromised user accounts. They've asked you to look at three Azure AD features, which one should you recommend?

■ Identity protection.

☐ Conditional access.

☐ Entitlement management.

Explanation
Identity protection is a tool that allows organizations to utilize security signals to identify potential threats.

Module 3 Describe the capabilities of Microsoft security solutions

Describe the basic security capabilities in Azure

Introduction

The traditional network security perimeter is changing as more companies move to either a hybrid cloud environment, with some resources located on-premises and some in the cloud, or a fully cloud-based network solution. Protection of your organization's assets, resources, and data is essential.

Threats can come from any direction: for instance, a Denial of Service attack on your organization's services, or a hacker trying to access your network by attempting to penetrate your firewall. Azure offers a wide array of configurable security tools that can be customized to give you the security and control to meet your organization's needs.

In this lesson, you'll explore many different services and features of Azure that can help protect your networks, assets, and resources, including DDoS protection, Azure Firewall, network security groups, and more. You'll also look at the different ways in which encryption is used to protect your data.

After completing this lesson, you should be able to:

- Describe Azure security capabilities for protecting your network.
- Describe how Azure can protect your VMs.
- Describe how encryption on Azure can protect your data.

Describe Azure DDoS protection

Any company, large or small, can be the target of a serious network attack. The nature of these attacks might be to make a statement, or simply because the attacker wanted a challenge.

Distributed Denial of Service attacks

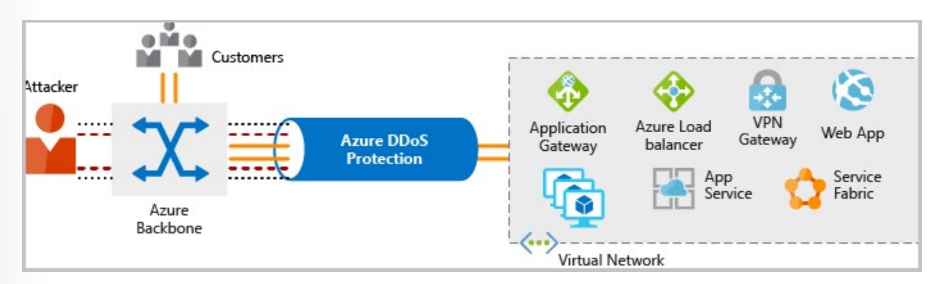
The aim of a Distributed Denial of Service (DDoS) attack is to overwhelm the resources on your applications and servers, making them unresponsive or slow for genuine users. A DDoS attack will usually target any public-facing device that can be accessed through the internet.

The three most frequent types of DDoS attack are:

- **Volumetric attacks**: These are volume-based attacks that flood the network with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through. These types of attacks are measured in bits per second.
- **Protocol attacks**: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols. These types of attacks are typically measured in packets per second.
- **Resource (application) layer attacks**: These attacks target web application packets, to disrupt the transmission of data between hosts.

What is Azure DDoS Protection?

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anything that looks like a DDoS attack.



In the diagram above, Azure DDoS Protection identifies an attacker's attempt to overwhelm the network. It blocks traffic from the attacker, ensuring that it doesn't reach Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.

Azure DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. During a DDoS attack, Azure can scale your computing needs to meet demand. DDoS Protection manages cloud consumption by ensuring that your network load only reflects actual customer usage.

Azure DDoS Protection comes in two tiers:

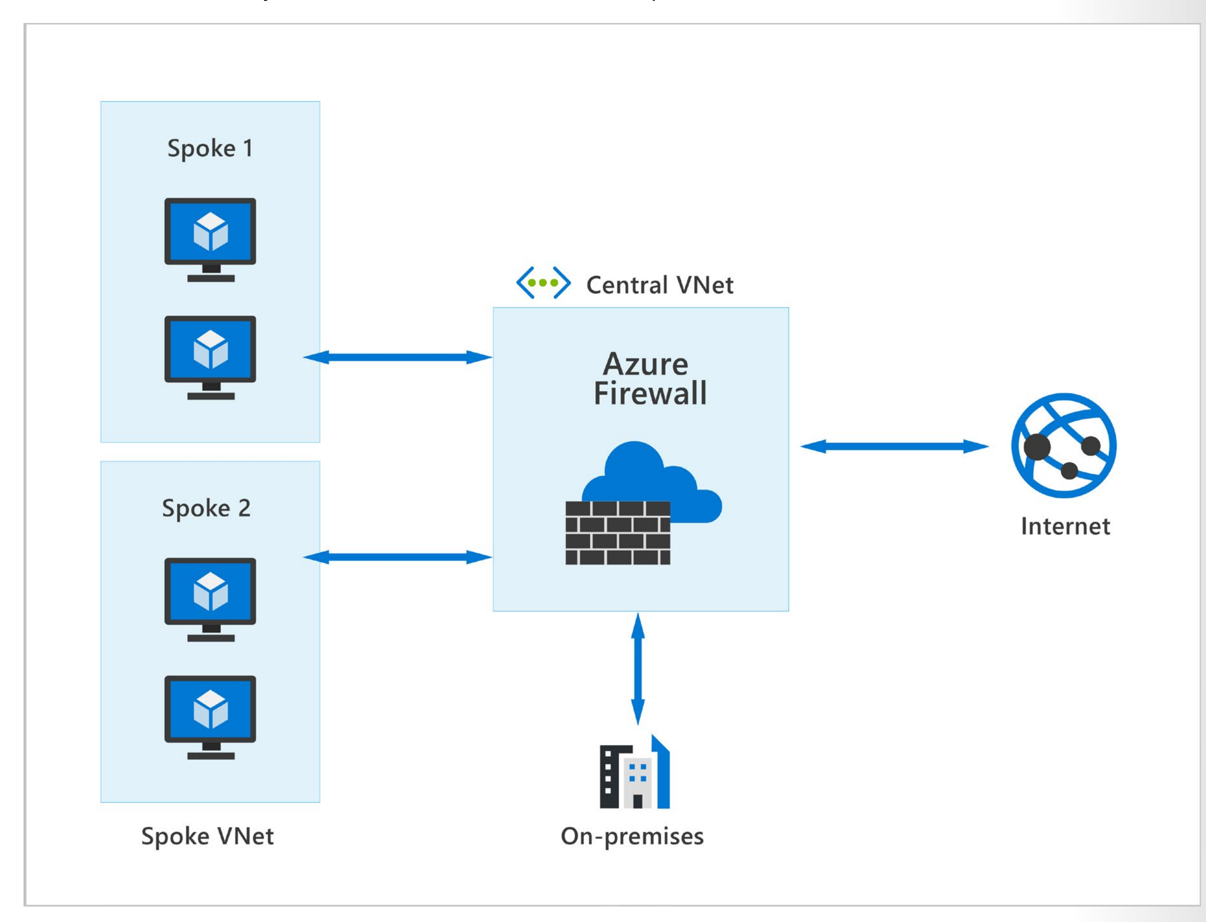
- **Basic**: The Basic service tier is automatically enabled for every property in Azure, at no extra cost, as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.
- **Standard**: The Standard service tier provides extra mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway.

  The DDoS Standard Protection service has a fixed monthly charge that includes protection for 100 resources. Protection for additional resources are charged on a monthly per-resource basis.

Use Azure DDoS to protect your devices and applications by analyzing traffic across your network, and taking appropriate action on suspicious traffic.

Describe Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure virtual network (VNet) resources from attackers. You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions.



With Azure Firewall, you can scale up the usage to accommodate changing network traffic flows, so you don't need to budget for peak traffic. Network traffic is subjected to the configured firewall rules when you route it to the firewall as the subnet default gateway.

Key features of Azure Firewall

Azure Firewall comes with many features, including but not limited to:

- **Built-in high availability and availability zones**: High availability is built in so there's nothing to configure. Also, Azure Firewall can be configured to span multiple availability zones for increased availability.
- **Network and application level filtering**: Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls.

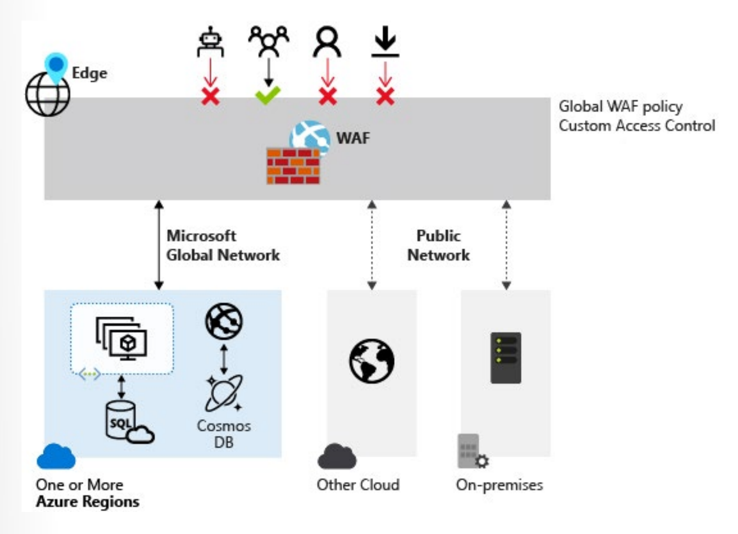
- **Outbound SNAT and inbound DNAT to communicate with internet resources**: Translate the private IP address of network resources to an Azure public IP address (source network address translation or SNAT) to identify and allow traffic originating from the virtual network to internet destinations. Similarly, inbound internet traffic to the firewall public IP address is translated (Destination Network Address Translation or DNAT) and filtered to the private IP addresses of resources on the virtual network.
- **Multiple public IP addresses**: These addresses can be associated with Azure Firewall.
- **Threat intelligence**: Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.
- **Integration with Azure Monitor**: Integrated with Azure Monitor to enable collecting, analyzing, and acting on telemetry from Azure Firewall logs.

Use Azure Firewall to help protect the Azure resources you've connected to Azure Virtual Networks.

Describe Web Application Firewall

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.



Describe network segmentation in Azure VNet

Segmentation is about dividing something into smaller pieces. An organization, for example, will typically consist of smaller business groups such as human resources, sales, customer service, and more. In an office environment, it's common to see each business group have their own dedicated office space, while members of the same group share an office. This enables members of the same business group to collaborate, while maintaining separation from other groups to address the confidentiality requirements of each business.

The same concept applies with corporate IT networks. The main reasons for network segmentation are:

- The ability to group related assets that are a part of (or support) workload operations.
- Isolation of resources.
- Governance policies set by the organization.

Network segmentation also supports the Zero Trust model and a layered approach to security that is part of a defense in depth strategy.

Assume breach is a principle of the Zero Trust model so the ability to contain an attacker is vital in protecting information systems. When workloads (or parts of a given workload) are placed into separate segments, you can control traffic from/to those segments to secure communication paths. If one segment is compromised, you'll be able to better contain the impact and prevent it from laterally spreading through the rest of your network.

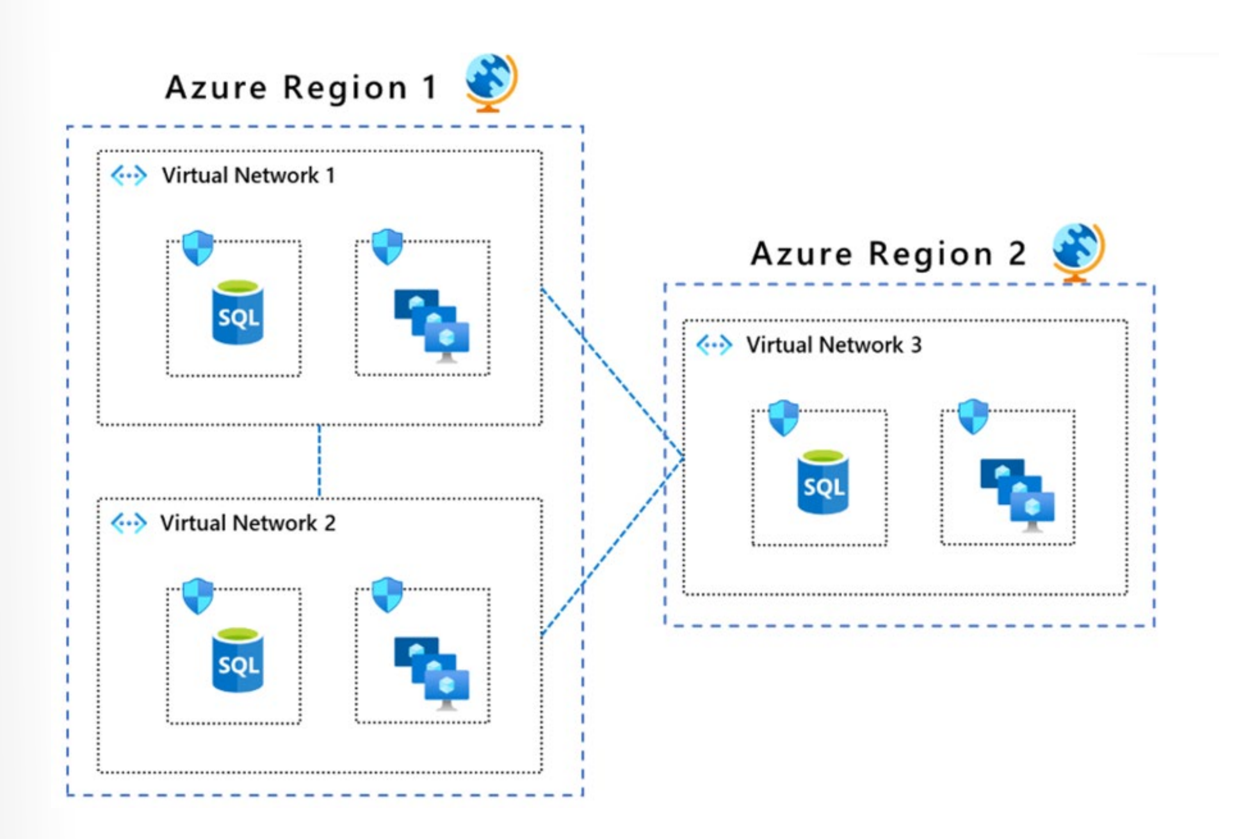
Network segmentation can secure interactions between perimeters. This approach can strengthen an organization's security posture, contain risks in a breach, and stop attackers from gaining access to an entire workload.

Azure Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your organization's private network in Azure. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Azure VNet enables organizations to segment their network. Organizations can create multiple VNets per region per subscription, and multiple smaller networks (subnets) can be created within each VNet.

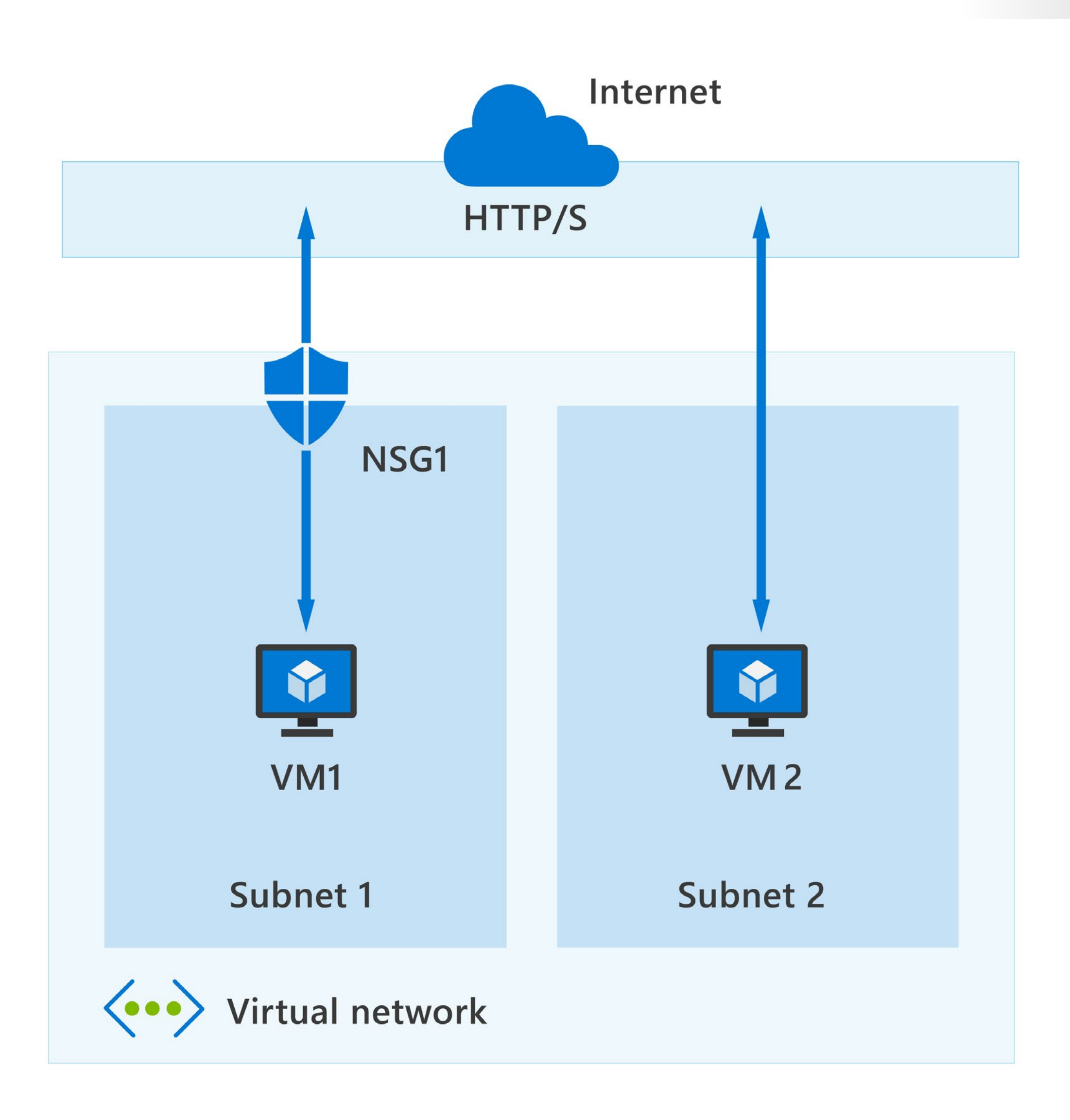
VNets provide network level containment of resources with no traffic allowed across VNets or inbound to the VNet, by default.   Communication needs to be explicitly provisioned. This enables more control over how Azure resources in a VNet communicate with other Azure resources, the internet, and on-premises networks.



Describe Azure Network Security groups

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine. An NSG consists of rules that define how the traffic is filtered. You can associate only one network security group to each virtual network subnet and network interface in a virtual machine. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

In the highly simplified diagram, shown below, you can see an Azure virtual network with two subnets that are connected to the internet, and each subnet has a virtual machine. Subnet 1 has an NSG assigned to it that's filtering inbound and outbound access to VM1, which needs a higher level of access. In contrast, VM2 could represent a public-facing machine that doesn't require an NSG.



Inbound and outbound security rules

An NSG is made up of inbound and outbound security rules. NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. By default, Azure creates a series of rules, three inbound and three outbound rules, to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Each rule specifies one or more of the following properties:

- **Name**: Every NSG rule needs to have a unique name that describes its purpose. For example, Admin-AccessOnlyFilter.
- **Priority**: Rules are processed in priority order, with lower numbers processed before higher numbers. When traffic matches a rule, processing stops. This means that any other rules with a lower priority (higher numbers) won't be processed.

- **Source or destination**: Specify either individual IP address or an IP address range, service tag (a group of IP address prefixes from a given Azure service), or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.
- **Protocol**: What network protocol will the rule check? The protocol can be any of: TCP, UDP, ICMP or Any.
- **Direction**: Whether the rule should be applied to inbound or outbound traffic.
- **Port range**: You can specify an individual or range of ports. Specifying ranges enables you to be more efficient when creating security rules.
- **Action**: Finally, you need to decide what will happen when this rule is triggered.

As an example, the table below shows the default inbound rules, which are included in all NSGs. For this example, assume no other inbound rules have been defined for this NSG.

Name	Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
Al-	65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow
AllowAzureLoadBalancerInBound	65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow
DenyAllInBound	65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

- The AllowVNetInBound rule is processed first as it has the lowest priority value. Recall that rules with the lowest priority value get processed first. This rule allows traffic from any Virtual Network (as defined by the VirtualNework service tag) on any port to any Virtual Network on any port, using any protocol. If a match is found for this rule, then no other rules are processed. If no match is found, then the next rule gets processed.
- The AllowAzureLoadBalancerInBound rule is processed second, as its priority value is higher than the AllowVNetInBound rule. This rule allows traffic from any Azure Load Balancer (as defined by the AzureLoadBalancer service tag) on any port to any IP address on any port, using any protocol. If a match is found for this rule, then no other rules are processed. If no match is found, then the next rule gets processed.
- The last rule in this NSG is the DenyAllInBound rule. This rule denies all traffic from any source IP address on any port to any other IP address on any port, using any protocol.

In summary, any virtual network subnet or network interface card to which this NSG is assigned will only allow inbound traffic from an Azure Virtual Network or an Azure load balancer. All other inbound network traffic is denied. Although not shown in this example, there are also three default outbound rules that are included in all NSGs. You can't remove the default rules, but you can override them by creating new rules with higher priorities (lower priority value).

What is the difference between Network Security Groups (NSGs) and Azure Firewall?

Now that you've learned about both Network Security Groups and Azure Firewall, you may be wondering how they differ, as they both protect Virtual Network resources. The Azure Firewall service complements network security group functionality. Together, they provide better “defense-in-depth” network security.

Network security groups provide distributed network layer traffic filtering to limit traffic to resources ***within*** virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network and application-level protection ***across*** different subscriptions and virtual networks.

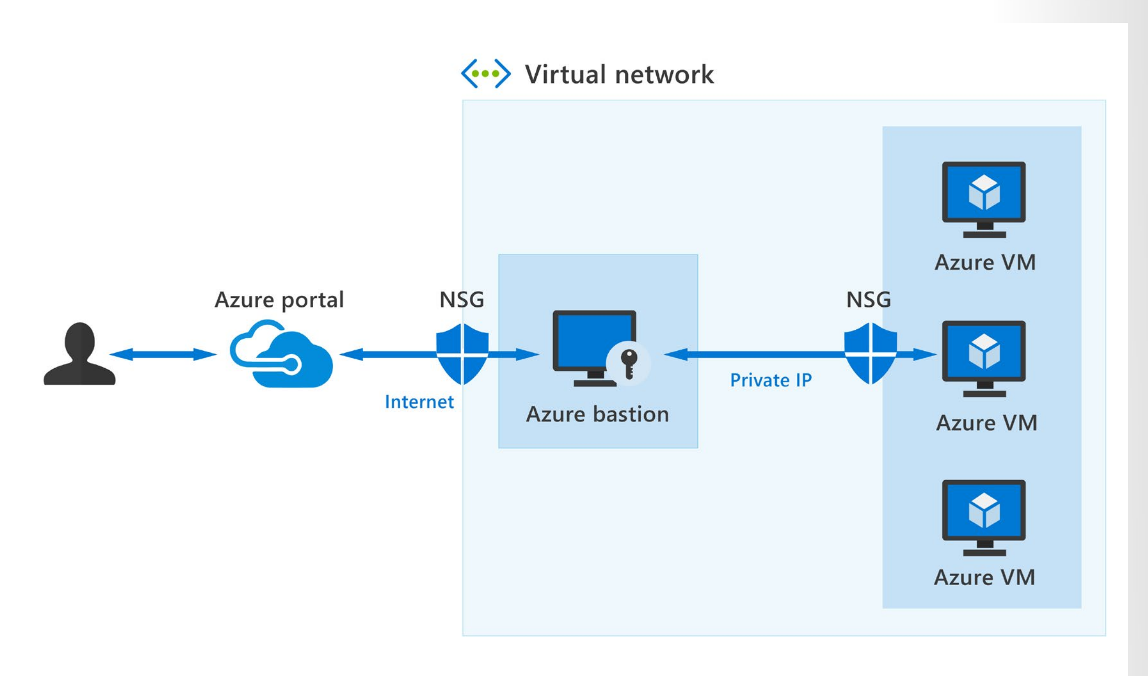
Describe Azure Bastion and Just-in-Time Access

Let's assume you've set up multiple virtual networks that use a combination of NSGs and Azure Firewalls to protect and filter access to the assets and resources, including virtual machines (VMs). You're now protected from external threats, but need to allow your developers and data scientist, who are working remotely, direct access to those VMs.

In a traditional model, you'd need to expose the Remote Desktop Protocol (RDP) and/or Secure Shell (SSH) ports to the internet. These protocols can be used to gain remote access to your VMs. This process creates a significant surface threat that can be exploited by attackers who actively hunt accessible machines with open management ports, like RDP or SSH. When a VM is successfully compromised, it's used as the entry point to attack further resources within your environment.

Azure Bastion

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.



Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network, and peered virtual networks, in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine. Once you provision the Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same VNet, as well as peered VNets.

Key features of Azure Bastion

The following features are available:

- **RDP and SSH directly in Azure portal**: You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.
- **Remote session over TLS and firewall traversal for RDP/SSH**: From the Azure portal, a connection to the VM, will open an HTML5 based web client that is automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely. The connection is made secure by using the Transport Layer Security (TLS) protocol to establish encryption.
- **No Public IP required on the Azure VM**: Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.
- **No hassle of managing NSGs**: A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.
- **Protection against port scanning**: Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.
- **Hardening in one place to protect against zero-day exploits**: Azure Bastion is a fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don’t need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

Use Azure Bastion to establish secure RDP and SSH connectivity to your virtual machines in Azure.

Just-in-time access

Just-in-time (JIT) access allows lock down of the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

When you enable just-in-time VM access, you can select the ports on the VM to which inbound traffic will be blocked. Microsoft Defender for Cloud, a tool for security posture management and threat protection, ensures “deny all inbound traffic” rules exist for your selected ports in the network security group (NSG) and Azure Firewall rules. These rules restrict access to your Azure VMs’ management ports and defend them from attack.

If other rules already exist for the selected ports, then those existing rules take priority over the new “deny all inbound traffic” rules. If there are no existing rules on the selected ports, then the new rules take top priority in the NSG and Azure Firewall.

Describe ways Azure encrypts data

Espionage, data theft, and data exfiltration are a real threat to any company. The loss of sensitive data can be crippling and have legal implications. For most organizations, data is their most valuable asset. In a layered security strategy, the use of encryption serves as the last and strongest line of defense.

Encryption on Azure

Microsoft Azure provides many different ways to secure your data, each depending on the service or usage required.

- **Azure Storage Service Encryption** helps to protect data at rest by automatically encrypting before persisting it to Azure-managed disks, Azure Blob Storage, Azure Files, or Azure Queue Storage, and decrypts the data before retrieval.
- **Azure Disk Encryption** helps you encrypt Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and data disks.
- **Transparent data encryption (TDE)** helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

What is Azure Key Vault?

Azure Key Vault is a centralized cloud service for storing your application secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities. It's useful for different kinds of scenarios:

- **Secrets management**. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
- **Key management**. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- **Certificate management**. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for Azure, and internally connected, resources more easily.
- **Store secrets backed by hardware security modules (HSMs)**. The secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Use the various ways in which Azure can encrypt your data to help you secure it whatever the location or state.

Knowledge check

Multiple choice

Item 1. The security admin has created an Azure Network Security Group (NSG) to filter network traffic to a virtual machine. The admin wants to allow inbound traffic using the Remote Desktop Protocol (RDP), but the default NSG rules are currently blocking all inbound traffic that is not from another virtual network or an Azure load balancer. What does the security admin have to do to allow inbound traffic using RDP?

☐ Delete the default rule.

☐ Create a new network security rule that allows RDP traffic and that has a higher priority than the default rule.

☐ There is nothing the admin can do, RDP traffic is not supported with NSGs.

Multiple choice

Item 2. The security admin wants to protect Azure resources from DDoS attacks, which Azure DDoS Protection tier will the admin use to target Azure Virtual Network resources?

- ☐ Basic.
- ☐ Standard.
- ☐ Advanced.

Multiple choice

Item 3. Your organization has several virtual machines in Azure. The security admin wants to deploy Azure Bastion to get secure access to the virtual machines in Azure. What should the admin keep in mind?

- ☐ Azure Bastion is deployed per virtual network, with support for virtual network peering.
- ☐ Azure Bastion is deployed per subscription.
- ☐ Azure Bastion is deployed per virtual machine.

Multiple choice

Item 4. Much of your organization's application data is in Azure. The security admin wants to take advantage of the encryption capabilities in Azure, which service would the admin use to store the application's secrets?

- ☐ Transparent data encryption.
- ☐ Secrets management.
- ☐ Azure Key Vault.

Summary and resources

The traditional network security perimeter protects your organization's assets, resources, where data is essential. Azure offers a wide range of configurable security tools that are customized to give the security and control to meet your organization's needs.

You've explored the different service offerings provided by Microsoft Azure, including DDoS protection, Azure Firewall, network security groups, Bastion, and others to protect access to your systems. You now understand the importance and use of encryption of data not only when stored, but also when in transit.

Without these security tools, your organization would be vulnerable to data theft, unable to respond swiftly to malicious attacks on your web and data services, and wouldn't meet your security obligations.

Now that you've completed this lesson, you should be able to:

- Describe Azure's security capabilities for protecting your network.
- Describe how Azure can protect your VMs.
- Describe how encryption on Azure can protect your data.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Azure DDoS Protection Standard overview**[1]
- **Azure DDoS Protection pricing page**[2]
- **Azure Firewall**[3]
- **Web Application firewall**[4]
- **What is Azure Virtual Desktop?**[5]
- **Network Security Groups**[6]
- **Azure Bastion**[7]
- **Understanding just-in-time (JIT) VM access**[8]
- **Encryption**[9]

1 https://docs.microsoft.com/azure/ddos-protection/ddos-protection-overview
2 https://azure.microsoft.com/pricing/details/ddos-protection/
3 https://docs.microsoft.com/azure/firewall/
4 https://docs.microsoft.com/azure/web-application-firewall/
5 https://docs.microsoft.com/azure/virtual-desktop/overview
6 https://docs.microsoft.com/azure/virtual-network/network-security-groups-overview
7 https://docs.microsoft.com/azure/bastion/
8 https://docs.microsoft.com/azure/defender-for-cloud/just-in-time-access-overview
9 https://docs.microsoft.com/learn/modules/intro-to-security-in-azure/4-encryption

Describe the security management capabilities of Azure

Introduction

As more companies move their assets and resources into the cloud, keeping them safe is a primary consideration for all IT and security departments. Cybercrime is a multi-billion-dollar business. Failure to protect your organization can be costly because of loss of data and reputation.

Microsoft Azure offers a suite of threat protection and detection systems to minimize and mitigate threats across your whole estate and improve the overall cloud security posture.

In this lesson, you'll learn about cloud security posture management (CSPM), explore the capabilities of Microsoft Defender for Cloud, including secure score. You'll also learn about the enhanced security capabilities of Microsoft Defender for Cloud. Finally, you'll learn about the Azure Security Benchmark and security baseline in Azure.

After completing this lesson, you'll be able to:

- Describe cloud security posture management.
- Describe the capabilities of Microsoft Defender for Cloud
- Understand the Azure Security Benchmark and security baseline in Azure.

Describe Cloud security posture management

Cloud-based systems are continually evolving and changing as companies move away from on-premises to the cloud. This move makes it difficult for any IT department to know if your data, assets, and resources are as fully protected as they used to be. Even a small misconfiguration of a new feature can increase the attack surface available for cybercriminals to exploit.

Cloud security posture management (CSPM) is a relatively new class of tools designed to improve your cloud security management. It assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud environment to monitor and prioritize security enhancements and features.

CSPM uses a combination of tools and services:

- **Zero Trust-based access control**: Considers the active threat level during access control decisions.
- **Real-time risk scoring**: To provide visibility into top risks.
- **Threat and vulnerability management (TVM)**: Establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.
- **Discover risks**: To understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.
- **Technical policy**: Apply guardrails to audit and enforce the organization's standards and policies to technical systems.
- **Threat modeling systems and architectures**: Used alongside other specific applications.

The main goal for a cloud security team working on posture management is to continuously report on and improve the organization's security posture by focusing on disrupting a potential attacker's return on investment (ROI).

The function of CSPM in your organization might be spread across multiple teams, or there may be a dedicated team. CSPM can be useful to many teams in your organization:

- Threat intelligence team
- Information technology
- Compliance and risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

Use CSPM to improve your cloud security management by assessing the environment, and automatically alerting security staff for vulnerabilities.

Describe Microsoft Defender for Cloud

Microsoft Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

Microsoft Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- **Continuously assess** - Know your security posture, identify and track vulnerabilities.
- **Secure** - Harden all connected resources and services.
- **Defend** - Detect and resolve threats to resources, workloads, and services.

The features of Microsoft Defender for Cloud, that deliver on these requirements, cover two broad pillars of cloud security: cloud security posture management and cloud workload protection.

Cloud security posture management (CSPM)

In Microsoft Defender for Cloud, the posture management features provide:

- Visibility - to help you understand your current security situation
- Hardening guidance - to help you efficiently and effectively improve your security

Visibility and hardening recommendations

The central feature in Microsoft Defender for Cloud that enables you to achieve those goals is secure score. Microsoft Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

Microsoft Defender for Cloud also provides hardening recommendations based on any identified security misconfigurations and weaknesses. Recommendations are grouped into security controls. Each control is a logical group of related security recommendations, and reflects your vulnerable attack surfaces. Your score only improves when you remediate all of the recommendations for a single resource within a control. Use these security recommendations to strengthen the security posture of your organization's Azure, hybrid, and multi-cloud resources.



Controls	Potential score increase	Unhealthy resources	Resource Health
Remediate vulnerabilities	+ 10% (6 points)	171 of 219 resources	
Enable encryption at rest	+ 5% (3 points)	147 of 231 resources	
Manage access and permissions	+ 5% (3 points)	20 of 36 resources	
Remediate security configurations	+ 4% (3 points)	134 of 212 resources	
Protect applications against DDoS attacks	+ 3% (2 points)	14 of 156 resources	
Encrypt data in transit	+ 3% (2 points)	135 of 331 resources	
Apply system updates	+ 3% (2 points)	57 of 212 resources	
Apply adaptive application control	+ 2% (1 point)	75 of 165 resources	
Secure management ports	+ 2% (1 point)	14 of 151 resources	
Apply data classification	+ 2% (1 point)	16 of 53 resources	
Restrict unauthorized network access	+ 1% (1 point)	48 of 241 resources	
Enable endpoint protection	+ 1% (1 point)	75 of 192 resources	
Enable auditing and logging	+ 1% (1 point)	134 of 180 resources	
Implement security best practices	+ 0% (0 points)	168 of 797 resources	
Enable advanced threat protection	+ 0% (0 points)	8 of 11 resources	
Custom recommendations	+ 0% (0 points)	1033 of 2183 resources	
Enable MFA *Completed*	+ 0% (0 points)	None	

In the following interactive guide you can explore how to use secure score and the hardening recommendations in Microsoft Defender for Cloud. Select the link below to get started and follow the prompts on the screen.

Interactive guide - Explore secure score[10]

Cloud workload protection (CWP)

The second pillar of cloud security is cloud workload protection. Through cloud workload protection capabilities, Microsoft Defender for Cloud is able to detect and resolve threats to resources, workloads, and services. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads. These are described in the next unit.

10 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP03M02-Use-Azure-secure-score-to-improve-your-security-posture/index.html?azure-portal=true

Describe the enhanced security of Microsoft Defender for Cloud

Microsoft Defender for Cloud is offered in two modes:

- Microsoft Defender for Cloud (Free) - Microsoft Defender for Cloud is enabled for free on all your Azure subscriptions. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.
- Microsoft Defender for Cloud with enhanced security features - Enabling enhanced security extends the capabilities of the free mode to workloads running in Azure, hybrid, and other cloud platforms, providing unified security management and threat protection across your workloads. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads.

Defender plans

Microsoft Defender for Cloud includes a range of advanced intelligent protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. The Microsoft Defender for Cloud plans you can select from are:

- **Microsoft Defender for servers** adds threat detection and advanced defenses for your Windows and Linux machines.
- **Microsoft Defender for App Service** identifies attacks targeting applications running over App Service.
- **Microsoft Defender for Storage** detects potentially harmful activity on your Azure Storage accounts.
- **Microsoft Defender for SQL** secures your databases and their data wherever they're located.
- **Microsoft Defender for Kubernetes** provides cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.
- **Microsoft Defender for container registries** protects all the Azure Resource Manager based registries in your subscription.
- **Microsoft Defender for Key Vault** is advanced threat protection for Azure Key Vault.
- **Microsoft Defender for Resource Manager** automatically monitors the resource management operations in your organization.
- **Microsoft Defender for DNS** provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.
- **Microsoft Defender for open-source relational protections** brings threat protections for open-source relational databases.

These different plans can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment.

Enhanced security features

Microsoft Defender plans specific to the types of resources in your subscriptions provide enhanced security features for your workloads. Listed below are some of the enhanced security features.

- Comprehensive endpoint detection and response - Microsoft Defender for servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR).
- Vulnerability scanning for virtual machines, container registries, and SQL resources - Easily deploy a scanner to all of your virtual machines. View, investigate, and remediate the findings directly within Microsoft Defender for Cloud.
- Multi-cloud security - Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features.
- Hybrid security – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.
- Threat protection alerts - Monitor networks, machines, and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.
- Track compliance with a range of standards - Microsoft Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark. When you enable the enhanced security features, you can apply a range of other industry standards, regulatory standards, and benchmarks according to your organization's needs. Add standards and track your compliance with them from the regulatory compliance dashboard.
- Access and application controls - Block malware and other unwanted applications by applying machine learning powered recommendations adapted to your specific workloads to create allowlists and blocklists. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs. Access and application controls drastically reduce exposure to brute force and other network attacks.

Additional benefits include threat protection for the resources connected to the Azure environment and container security features, among others. Some features may be associated with specific defender plans for specific workloads.

Describe Azure Security Benchmark and security baselines for Azure

New services and features are released daily in Azure, developers are rapidly publishing new cloud applications built on these services, and attackers are always seeking new ways to exploit misconfigured resources.

The Azure Security Benchmark (ASB) and security baselines for Azure, which are closely related, help organizations secure their cloud solutions on Azure.

The Azure Security Benchmark

Microsoft has found that using security benchmarks can help organizations quickly secure their cloud deployments and reduce risk to their organization.

The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. The best way to understand the Azure Security Benchmark is to view it on GitHub **Azure Security Benchmark V3**[11]. Spoiler alert, it's an excel spreadsheet. Some of the key pieces of information in ASB V3 are:

- ASB ID - Each line item in the ASB has an identifier that maps to a specific recommendation.
- Control domain - ASB control domains include network security, data protection, identity management, privileged access, incident response, endpoint security to name just a few. The control domain is best described as high-level feature or activity that isn't specific to a technology or implementation.
- Mapping to industry frameworks - The recommendations included in the ASB map to existing industry frameworks, such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standards (PCI DSS) frameworks. This makes security and compliance easier for customer applications running on Azure services.
- Recommendation - For each control domain area there can be many distinct recommendations. Each recommendation captures specific functionality associated with the control domain area and is itself a control. For example, the "Network Security" control domain in ASB v3 has 10 distinct recommendations identified as NS-1 through NS-10. Each of these recommendations describes a specific control under network security.
- Security principle - Each recommendation lists a "Security Principle" that explains the "what" for the control at the technology-agnostic level
- Azure Guidance - Azure Guidance is focused on the "how", elaborating on the relevant technical features and ways to implement the controls in Azure.

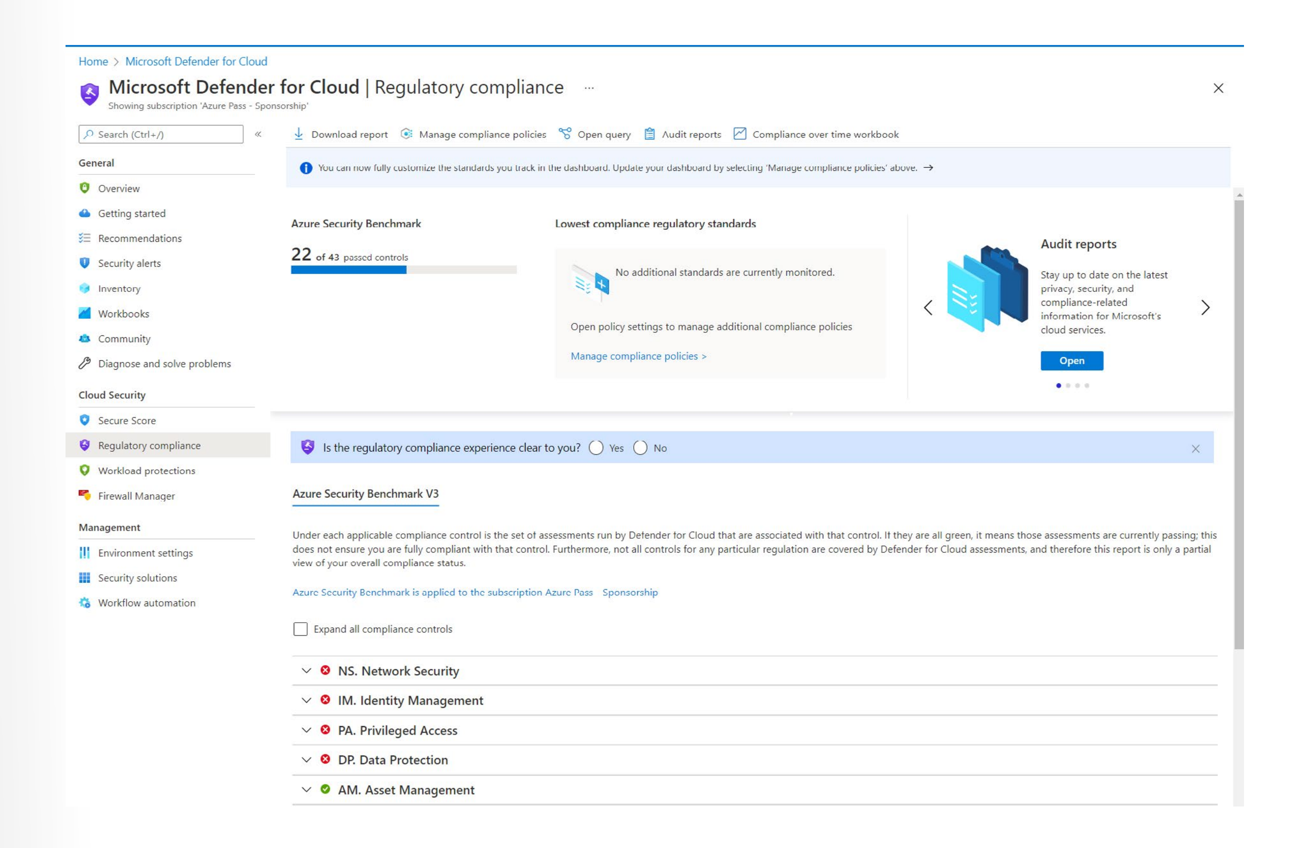
Other pieces of information in the ASB include links to information on implementation, links to information about security stakeholders, and guidance on mapping to Azure policy. The image below is an excerpt from the Azure Security Benchmark (ASB v3) and is shown as an example of the type of the content that is included in the ASB v3. The image is not intended to show the complete text for any of the line items.

Mapping to industry frameworks

ASB ID	Control Domain	CIS Controls v7.1 ID(s)	CIS Controls v8 ID(s)	NIST SP800-53 r4 ID(s)	PCI-DSS v3.2.1 ID(s)	Recommendation	Security Principle	Azure Guidance
NS-1	Network Security	9.2 - Ensure Only Approved Ports, Protocols and Services Are Running 9.4 - Apply Host-Based Firewalls or Port Filtering 12.3 - Deny Communications with Known Malicious IP	3.12 - Segment Data Processing and Storage Based on Sensitivity 13.4 - Perform Traffic Filtering Between Network Segments 4.4 - Implement and Manage a Firewall on Severs	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Establish network segmentation boundaries	Ensure that your virtual network deployment aligns to your enterprise segmentation strategy defined in the GS-2 security control. Any workload that could incur higher risk for the organization should be in isolated virtual networks.	Create a virtual network (VNet) as a fundamental segmentation approach in your Azure network, so resources such as VMs can be deployed into the VNet within a network boundary. To further segment the network, you can create subnets inside VNet for smaller sub-networks.
NS-2	Network Security	14.1 - Segment the Network Based on Sensitivity	3.12 - Segment Data Processing and Storage Based on Sensitivity 4.4 - Implement and Manage a Firewall on Servers	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Secure cloud services with network controls	Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access from public network when possible.	Deploy private endpoints for all Azure resources that support the Private Link feature, to establish a private access point for the resources. You should also disable or restrict public network access to services where feasible.

Microsoft Defender for Cloud continuously assesses an organization's hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark. Some of the controls used in the ASB include network security, identity and access control, data protection, data recovery, incident response, and more.

11 https://github.com/MicrosoftDocs/SecurityBenchmarks/tree/master/Azure%20Security%20Benchmark/3.0



Security baselines for Azure

Security baselines for Azure apply guidance from the Azure Security Benchmark to the specific service for which it's defined. For example, the security baseline for Azure Active Directory applies guidance from the Azure Security Benchmark version 2.0 to Azure Active Directory.

Security baselines for Azure help organizations strengthen their security through improved tooling, tracking, and security features. They also provide organizations a consistent experience when securing their environment. Content in the security baseline is grouped by the control domains defined by the Azure Security Benchmark and that are applicable to the service.

Each Azure security baseline includes the following information:

- **Azure ID**: The Azure Security Benchmark ID that corresponds to the recommendation.
- **Azure control**: The content is grouped by control domain area, as listed in the Azure Security Benchmark, and that is applicable to the service for which the security baseline is defined.
- **Benchmark Recommendation**: This maps to the recommendation for the associated ASB ID (or Azure ID). Each recommendation describes an individual control in a control domain.
- **Customer Guidance**: The rationale for the recommendation and links to guidance on how to implement it.
- **Responsibility**: Who is responsible for implementing the control? Possible scenarios are customer responsibility, Microsoft responsibility, or shared responsibility.
- **Microsoft Defender for Cloud monitoring**: Does Microsoft Defender for Cloud monitor the control?

The image below is an excerpt from the security baseline for Azure AD and is shown as an example of the type of the content that is included in baseline. The image is not intended to show the complete text for any of the line items.

Service	Azure Control	Azure ID	Benchmark Recommendation	Customer Guidance	Responsibility	Microsoft Defender for Cloud Monitoring
Azure Active Directory	Network Security	NS-6	Simplify network security rules	Use Azure Virtual Network Service Tags to define network access controls on network security groups or Azure Firewall configured for your Azure Active Directory resources.	Customer	Not applicable
Azure Active Directory	Network Security	NS-7	Secure Domain Name Service (DNS)	Azure Active Directory does not expose its underlying DNS configurations; these settings are maintained by Microsoft.	Microsoft	Not applicable

Refer to **Azure Security Benchmark documentation**[12] for a complete listing of the available baselines.

Knowledge check

Multiple choice

Item 1. An organization is using Azure and wants to improve their security best practices. Which Azure specific benchmark would the IT security team need to consider?

☐ Azure Security Benchmark.

☐ Center for Internet Security.

☐ Microsoft cybersecurity group

Multiple choice

Item 2. Your organization is using Microsoft Defender for Cloud to assess your resources, subscriptions, and organization for security issues. Your organization's overall secure score is low and needs to improve. How would a security admin go about improving the score?

☐ Close old security recommendations.

☐ Remediate security recommendations.

☐ Move security recommendations to resolved.

Multiple choice

Item 3. An organization wants to add vulnerability scanning for its Azure resources to view, investigate, and remediate the findings directly within Microsoft Defender for Cloud. What functionality of Microsoft Defender for Cloud would they need to consider?

☐ Secure score and recommendations functionality that is part of the CSPM pillar of Microsoft Defender for Cloud.

☐ The enhanced functionality that is provided through the Microsoft Defender plans and is part of the CWP pillar of Microsoft Defender for Cloud.

☐ Security Benchmarks.

12 https://docs.microsoft.com/azure/security/benchmarks/

Summary and resources

Microsoft Azure offers a suite of threat protection and detection systems to minimize and mitigate threats across your whole estate and improve the overall cloud security posture.

You've learned about cloud security posture management (CSPM). You've also explored the capabilities of Microsoft Defender for Cloud and how to understand your security position using secure score. You've discovered the different plans of Microsoft Defender for Cloud that are available and the enhanced security benefits they offer. Finally, you've learned about the Azure Security Benchmark and security baseline in Azure.

Now that you've completed this lesson, you'll be able to:

- Describe cloud security posture management.
- Describe the capabilities of Microsoft Defender for Cloud
- Understand the Azure Security Benchmark and security baseline in Azure.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **What is Microsoft Defender for Cloud?**[13]
- **Secure score in Microsoft Defender for Cloud**[14]
- **Microsoft Defender for Cloud pricing**[15]
- **Azure Security Benchmark (v3)**[16]
- **Security baselines**[17]

13 https://docs.microsoft.com/azure/security-center/azure-defender
14 https://docs.microsoft.com/azure/security-center/secure-score-security-controls
15 https://azure.microsoft.com/pricing/details/azure-defender/
16 https://docs.microsoft.com/security/benchmark/azure/overview
17 https://docs.microsoft.com/azure/security/benchmarks/security-baselines-overview

Describe the security capabilities of Microsoft Sentinel

Introduction

Every organization, whatever its size, is susceptible to security threats and attacks. Being able to collect data to gain visibility into your digital estate and detect, investigate, and respond to threats is central to any network security strategy.

In this lesson, you'll learn about the different security defenses that are available to protect your company's digital estate. You'll explore how Microsoft Sentinel provides a single solution for alert detection, threat visibility, proactive hunting, and threat response. Finally, you'll have a high-level understanding of the pricing model of Microsoft Sentinel.

After completing this lesson, you'll be able to:

- Describe the security concepts for SIEM and SOAR.
- Describe how Microsoft Sentinel provides integrated threat protection.
- Describe the pricing models of Microsoft Sentinel.

Define the concepts of SIEM and SOAR

Protecting an organization's digital estate, resources, assets, and data from security breaches and attacks is an ongoing and escalating challenge. The business world has large numbers of staff working remotely, creating an exploitable window for cybercriminals.

Having a resilient and robust, industry-standard set of tools can help mitigate and prevent these exploits. Security information event management (SIEM) and security orchestration automated response (SOAR) provide security insights and security automation that can enhance an organization's threat visibility and response.

What is security information and event management (SIEM)?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

What is security orchestration automated response (SOAR)?

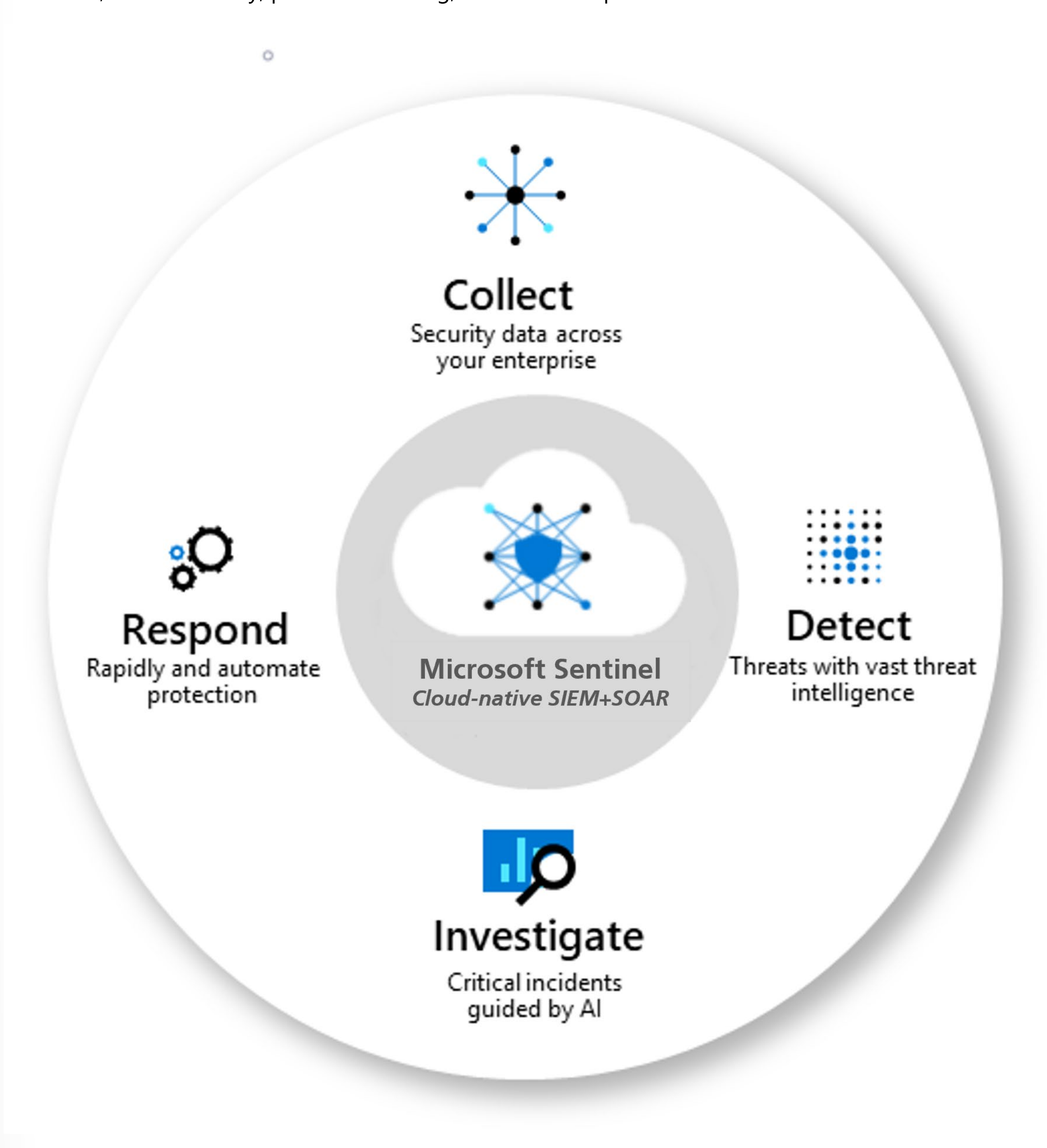
A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

To provide a comprehensive approach to security, an organization needs to use a solution that embraces or combines both SIEM and SOAR functionality.

Describe Microsoft Sentinel

Effective management of an organization's network security perimeter requires the right combination of tools and systems. Microsoft Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelli-

gent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.



This diagram shows the end-to-end functionality of Microsoft Sentinel.

- **Collect** data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.
- **Investigate** threats with artificial intelligence (AI) and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- **Respond** to incidents rapidly with built-in orchestration and automation of common security tasks.

Microsoft Sentinel helps enable end-to-end security operations, in a modern Security Operations Center (SOC). Listed below are some of the key features of Microsoft Sentinel.

Connect Sentinel to your data

To on-board Microsoft Sentinel, you first need to connect to your security sources. Microsoft Sentinel comes with many connectors for Microsoft solutions, available out of the box and providing real-time integration. Included are Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, and more. In addition, there are built-in connectors to the broader security ecosystem of non-Microsoft solutions. You can also connect your data sources using community-built data connectors listed in the Microsoft Sentinel GitHub repository or by following generic deployment procedures for how to connect your data source to Microsoft Sentinel. Links to information are included in the Learn more section of the summary and resources unit.

Workbooks

After you connect data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks. You'll see a canvas for data analysis and the creation of rich visual reports within the Azure portal. Through this integration, Microsoft Sentinel allows you to create custom workbooks across your data. It also comes with built-in workbook templates that allow quick insights across your data as soon as you connect a data source.

Analytics

Microsoft Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve. With analytics in Microsoft Sentinel, you can use the built-in correlation rules as-is, or use them as a starting point to build your own. Microsoft Sentinel also provides machine learning rules to map your network behavior and then look for anomalies across your resources. These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.

Manage incidents in Microsoft Sentinel

Incident management allows you to manage the lifecycle of the incident. View all related alerts that are aggregated into an incident. You can also triage and investigate. Review all related entities in the incident and additional contextual information meaningful to the triage process. Investigate the alerts and related entities to understand the scope of breach. Trigger playbooks on the alerts grouped in the incident to resolve the threat detected by the alert. You can also do standard incident management tasks like changing status or assigning incidents to individuals for investigation.

Security automation and orchestration

You can use Microsoft Sentinel to automate some of your security operations and make your security operations center (SOC) more productive. Microsoft Sentinel integrates with Azure Logic Apps, so you can create automated workflows, or playbooks, in response to events. A security playbook is a collection of procedures that can help SOC engineers and analysts of all tiers to automate and simplify tasks and orchestrate a response. Playbooks work best with single, repeatable tasks, and require no coding knowledge.

Investigation

Currently in preview, Microsoft Sentinel's deep investigation tools help you to understand the scope of a potential security threat and find the root cause. You choose an entity on the interactive graph to ask

specific questions, then drill down into that entity and its connections to get to the root cause of the threat.

Hunting

Use Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework (a global database of adversary tactics and techniques), to proactively hunt for security threats across your organization's data sources, before an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.

While hunting, you can bookmark interesting events enabling you to return to them later, share them with others, and group them with other correlating events to create a compelling incident for investigation.

Notebooks

Microsoft Sentinel supports Jupyter notebooks. Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. You can use Jupyter notebooks in Microsoft Sentinel to extend the scope of what you can do with Microsoft Sentinel data. For example, perform analytics that aren't built in to Microsoft Sentinel, such as some Python machine learning features, create data visualizations that aren't built in to Microsoft Sentinel, such as custom timelines and process trees, or integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Community

The Microsoft Sentinel community is a powerful resource for threat detection and automation. Microsoft security analysts constantly create and add new workbooks, playbooks, hunting queries, and more, posting them to the community for you to use in your environment. You can download sample content from the private community GitHub repository to create custom workbooks, hunting queries, notebooks, and playbooks for Microsoft Sentinel.

Microsoft Sentinel video presentation

In this video of **Microsoft Sentinel**[18], you'll explore many of the key features available in Microsoft Sentinel, including incidents, workbooks, hunting, notebooks, analytics, and playbooks.

Understand Microsoft Sentinel costs

Microsoft Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Billing is based on the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace. There are two ways to pay for the Microsoft Sentinel service: Capacity Reservations and Pay-As-You-Go.

- **Capacity Reservations**: With Capacity Reservations, you're billed a fixed fee based on the selected tier, enabling a predictable total cost for Microsoft Sentinel.
- **Pay-As-You-Go**: With Pay-As-You-Go pricing, you're billed per gigabyte (GB) for the volume of data ingested for analysis in Microsoft Sentinel and stored in the Azure Monitor Log Analytics workspace.

18 https://www.microsoft.com/videoplayer/embed/RE4LHLR

For more information on pricing and a free trial of Microsoft Sentinel on an Azure Monitor Log Analytics workspace, visit **Microsoft Sentinel pricing**[19].

Knowledge check

Multiple choice

Item 1. As the lead admin, it is important to convince your team to start using Microsoft Sentinel. You've put together a presentation. What are the four security operation areas of Microsoft Sentinel that cover this area?

☐ Collect, Detect, Investigate, and Redirect.

☐ Collect, Detect, Investigate, and Respond.

☐ Collect, Detect, Investigate, and Repair.

Multiple choice

Item 2. Your estate has many different data sources where data is stored. Which tool should be used with Microsoft Sentinel to quickly gain insights across your data as soon as a data source is connected?

☐ Azure Monitor Workbooks.

☐ Playbooks.

☐ Microsoft 365 Defender.

Summary and resources

In this lesson, you learned about the security defenses available to protect your company's digital estate. You also discovered the key security operation areas that Microsoft Sentinel supports and how it integrates with your existing security systems. You get a single solution for alert detection, threat visibility, proactive hunting, and threat response. You also learned about the two ways to pay for the Microsoft Sentinel service: Capacity Reservations and Pay-As-You-Go. Microsoft Sentinel's.

Now that you've completed this lesson, you'll be able to:

- Describe the security concepts for SIEM and SOAR.
- Describe how Microsoft Sentinel provides integrated threat protection.
- Describe the pricing models of Microsoft Sentinel.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Microsoft Sentinel and SIEM**[20]
- **What is Microsoft Sentinel?**[21]
- **Microsoft Sentinel pricing**[22]

19 https://azure.microsoft.com/pricing/details/azure-sentinel/
20 https://azure.microsoft.com/services/azure-sentinel/
21 https://docs.microsoft.com/azure/sentinel/overview
22 https://azure.microsoft.com/pricing/details/azure-sentinel/

Describe the threat protection capabilities of Microsoft 365 Defender

Introduction

Security threat prevention is not limited to just network security. It also covers applications, email, collaborations, endpoints, cross SaaS solutions, identity, and more. With the integrated Microsoft 365 Defender solution, security professionals can stitch together the threat signals that each of these products receive and determine the full scope and impact of the threat; how it entered the environment, what it's affected, and how it's currently impacting the organization.

In this lesson, you'll see how the Microsoft Defender service can help protect your organization. You'll explore each of the different defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps. You'll also explore the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, reports, and incident management.

After completing this lesson, you'll be able to:

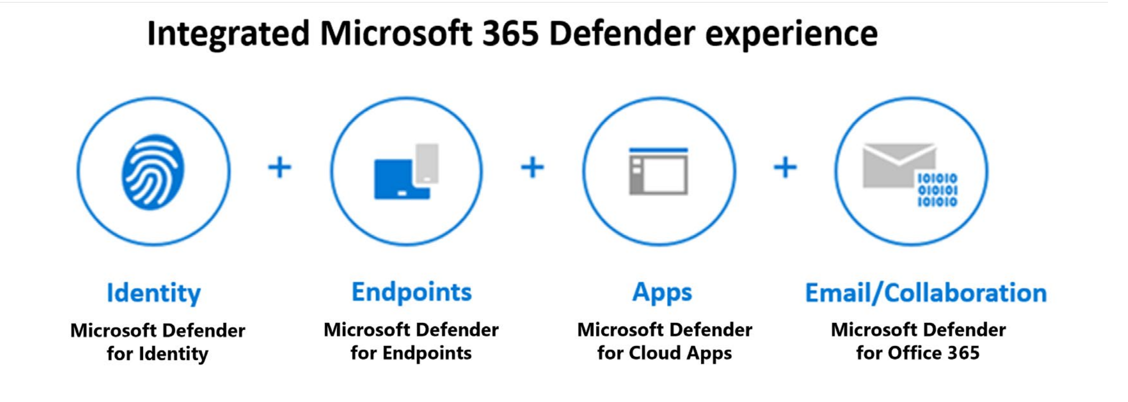
- Describe the Microsoft 365 Defender service.
- Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.
- Describe and explore Microsoft 365 Defender portal.

Describe Microsoft 365 Defender services

Microsoft 365 Defender is an enterprise defense suite that protects against sophisticated cyberattacks. With Microsoft 365 Defender, you can natively coordinate the detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications.

Refer to the **Microsoft 365 Defender overview**[23] for a video overview of Microsoft 365 Defender.

Microsoft 365 Defender allows admin's to assess threat signals from applications, email, and identity to determine an attack's scope and impact. It gives greater insight into how the threat occurred, what systems have been affected, and can take automated action to prevent or stop the attack.



23 https://www.microsoft.com/videoplayer/embed/RE4IPYr

Microsoft 365 Defender suite protects:

- **Identities with Microsoft Defender for Identity and Azure AD Identity Protection** - Microsoft Defender for Identity uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
- **Endpoints with Microsoft Defender for Endpoint** - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.
- **Applications with Microsoft Defender for Cloud Apps** - Microsoft Defender for Cloud Apps is a comprehensive cross-SaaS solution that brings deep visibility, strong data controls, and enhanced threat protection to your cloud apps.
- **Email and collaboration with Microsoft Defender for Office 365** - Defender for Office 365 safe-guards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools.

Use Microsoft Defender to protect your organization against sophisticated cyberattacks. It coordinates your detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications.

Describe Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Microsoft Defender for Office 365 covers these key areas:

- **Threat protection policies**: Define threat protection policies to set the appropriate level of protection for your organization.
- **Reports**: View real-time reports to monitor Microsoft Defender for Office 365 performance in your organization.
- **Threat investigation and response capabilities**: Use leading-edge tools to investigate, understand, simulate, and prevent threats.
- **Automated investigation and response capabilities**: Save time and effort investigating and mitigat-ing threats.

Microsoft Defender for Office 365 is available in two plans. The plan you choose influences the tools you’ll see and use. It's important to make sure you select the best plan to meet your organization's needs.

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and detection tools for your Office 365 suite:

- **Safe Attachments**: Checks email attachments for malicious content.
- **Safe Links**: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.
- **Safe Attachments for SharePoint, OneDrive, and Microsoft Teams**: Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.

- **Anti-phishing protection**: Detects attempts to impersonate your users and internal or custom domains.
- **Real-time detections**: A real-time report that allows you to identify and analyze recent threats.

Microsoft Defender for Office 365 Plan 2

This plan includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite:

- **Threat Trackers**: Provide the latest intelligence on prevailing cybersecurity issues, and allow an organization to take countermeasures before there's an actual threat.
- **Threat Explorer**: A real-time report that allows you to identify and analyze recent threats.
- **Automated investigation and response (AIR)**: Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.
- **Attack Simulator**: Allows you to run realistic attack scenarios in your organization to identify vulnerabilities. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.
- **Proactively hunt for threats with advanced hunting in Microsoft 365 Defender**: Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities.
- **Investigate alerts and incidents in Microsoft 365 Defender**: Microsoft Defender for Office 365 P2 customers have access to Microsoft 365 Defender integration to efficiently detect, review, and respond to incidents and alerts.

Microsoft Defender for Office 365 availability

Microsoft Defender for Office 365 is included in certain subscriptions, such as Microsoft 365 E5, Office 365 E5, Office 365 A5, and Microsoft 365 Business Premium.

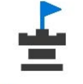
If your subscription doesn't include Defender for Office 365, you can purchase it as an add-on.

Use Microsoft 365 Defender for Office 365 to protect your organization's collaboration tools and messages.

Describe Microsoft Defender for Endpoint

Microsoft Defender for Endpoint, formerly Microsoft Defender Advanced Threat Protection, is a platform designed to help enterprise networks protect endpoints. It does so by preventing, detecting, investigating, and responding to advanced threats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and MSFT cloud services.

This technology includes endpoint behavioral sensors that collect and process signals from the operating system, cloud security analytics that turn signals into insights, detections and recommendations, and threat intelligence to identify attacker tools, techniques, generate alerts.









Microsoft Defender for Endpoint includes:

- **Threat and vulnerability management**: A risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. It uses sensors on devices to avoid the need for agents or scans, and prioritizes vulnerabilities.
- **Attack surface reduction**: Reduces the places where your organization is vulnerable to cyberthreats and attacks by ensuring only *allowed* apps can run, and preventing apps from accessing dangerous locations.
- **Next generation protection**: Brings together machine learning, big data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices in your enterprise organization.
- **Endpoint detection and response**: Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.
- **Automated investigation and remediation**: The automated investigation feature uses inspection algorithms and processes used by analysts (such as playbooks) to examine alerts and take quick remediation action to resolve breaches. This process significantly reduces the volume of alerts that must be investigated individually.
- **Microsoft Threat Experts**: A managed threat hunting service that provides Security Operation Centers (SOCs) with monitoring and analysis tools to ensure critical threats don’t get missed.
- **Management and APIs**: Provides APIs to integrate with other solutions.

Microsoft Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve overall security. Microsoft Defender for Endpoint integrates with various components in the Microsoft Defender suite, and with other Microsoft solutions including Intune and Microsoft Defender for Cloud.

Use Microsoft Defender for Endpoint to protect your organization's endpoints and respond to advanced threats.

Describe Microsoft Defender for Cloud Apps

Moving to the cloud increases flexibility for employees and IT teams. However, it also introduces new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance for supporting access while protecting critical data.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB). It's a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the cloud provider. Microsoft Defender for Cloud Apps provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Use this service to gain visibility into Shadow IT by discovering the cloud apps being used. You can control and protect data in the apps after you sanction them to the service.

What is a Cloud Access Security Broker?

A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use, wherever they're located, and regardless of the device they're using. CASBs help organizations protect their environment by providing a wide range of capabilities across the following pillars:

- **Visibility** - Detect cloud services and app use and provide visibility into Shadow IT.
- **Threat protection** - Monitor user activities for anomalous behaviors, control access to resources through access controls, and mitigate malware.
- **Data security** - Identify, classify and control sensitive information, protecting against malicious actors.
- **Compliance** - Assess the compliance of cloud services.

These capability areas represent the basis of the Defender for Cloud Apps framework described below.

The Defender for Cloud Apps framework

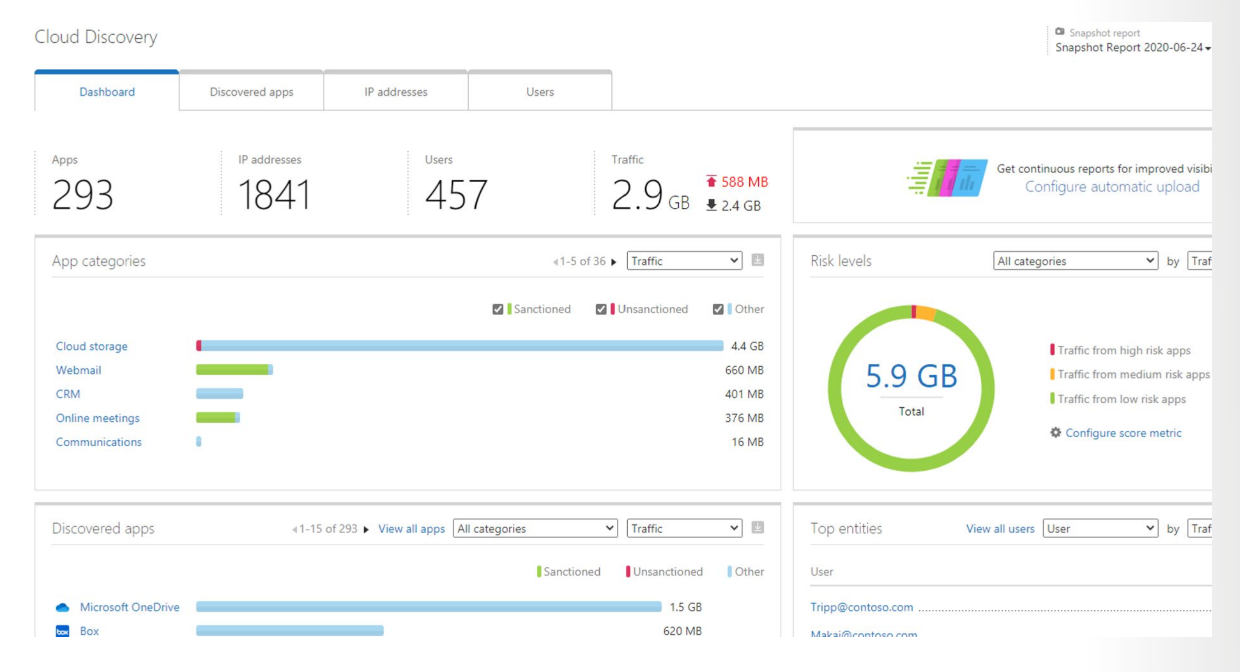
Microsoft Defender for Cloud Apps is built on a framework that provides the following capabilities:

- **Discover and control the use of Shadow IT**: Identify the cloud apps, and IaaS and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks.
- **Protect against cyberthreats and anomalies**: Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage, and remediate automatically to limit risks.
- **Protect your sensitive informationanywhere in the cloud**: Understand, classify, and protect the exposure of sensitive information at rest. Use out-of-the-box policies and automated processes to apply controls in real time across all your cloud apps.
- **Assess your cloud apps' compliance**: Assess if your cloud apps meet relevant compliance requirements, including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.

Microsoft Defender for Cloud Apps functionality

Defender for Cloud Apps Security delivers on the components of the framework through an extensive list of features and functionality. Listed below are some examples.

- **Cloud Discovery** maps and identifies your cloud environment and the cloud apps your organization uses. Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps being used.
- **Sanctioning and unsanctioning apps** in your organization by using the Cloud apps catalog that includes over 25,000 cloud apps. The apps are ranked and scored based on industry standards. You can use the cloud app catalog to rate the risk for your cloud apps based on regulatory certifications, industry standards, and best practices.
- Use **App connectors** to integrate Microsoft and non-Microsoft cloud apps with Microsoft Defender for Cloud Apps, extending control and protection. Defender for Cloud Apps queries the app for activity logs, and it scans data, accounts, and cloud content that can be used to enforce policies, detect threats and provide governance actions to resolve issues.
- **Conditional Access** App Control protection provides real-time visibility and control over access and activities within your cloud apps. Avoid data leaks by blocking downloads before they happen, setting rules to require data stored in and downloaded from the cloud to be protected with encryption, and controlling access from non-corporate or risky networks.
- Use **policies** to detect risky behavior, violations, or suspicious data points and activities in your cloud environment. You can use policies to integrate remediation processes to achieve risk mitigation.



Interactive Guide

In this interactive guide, you'll get an introduction to the capabilities available with Microsoft Defender for Cloud Apps. Select the link below to get started and follow the prompts on the screen.

Interactive guide - Explore Microsoft Defender for Cloud Apps[24]

24 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP03M04-Describe-threat-protection-with-Microsoft-365/index.html?azure-portal=true

Describe Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security solution. It uses your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Microsoft Defender for Identity provides security professionals managing hybrid environments functionality to:

- Monitor and profile user behavior and activities.
- Protect user identities and reduce the attack surface.
- Identify and investigate suspicious activities and advanced attacks across the cyberattack kill-chain.
- Provide clear incident information on a simple timeline for fast triage

Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence. It gives insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.

Protect user identities and reduce the attack surface

Defender for Identity provides insights on identity configurations and suggested security best practices. Through security reports and user profile analytics, Defender for Identity helps reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack.

Defender for Identity security reports, help identify users and devices that authenticate using clear-text passwords. It also provides extra insights into how to improve security posture and policies.

For hybrid environments in which Active Directory Federation Services (AD FS) is present, Defender for Identity protects the AD FS by detecting on-premises attacks and providing visibility into authentication events generated by the AD FS.

Identify suspicious activities and advanced attacks across the cyberattack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user. Attacks then quickly move laterally until the attacker accesses valuable assets. These assets might include sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill chain:

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance

Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Use the Defender for Identity attack timeline view and the intelligence of smart analytics to stay focused on what matters. Also, you can use Defender for Identity to quickly investigate threats, and gain insights across the organization for users, devices, and network resources.

Microsoft Defender for Identity protects your organization from compromised identities, advanced threats, and malicious insider actions.

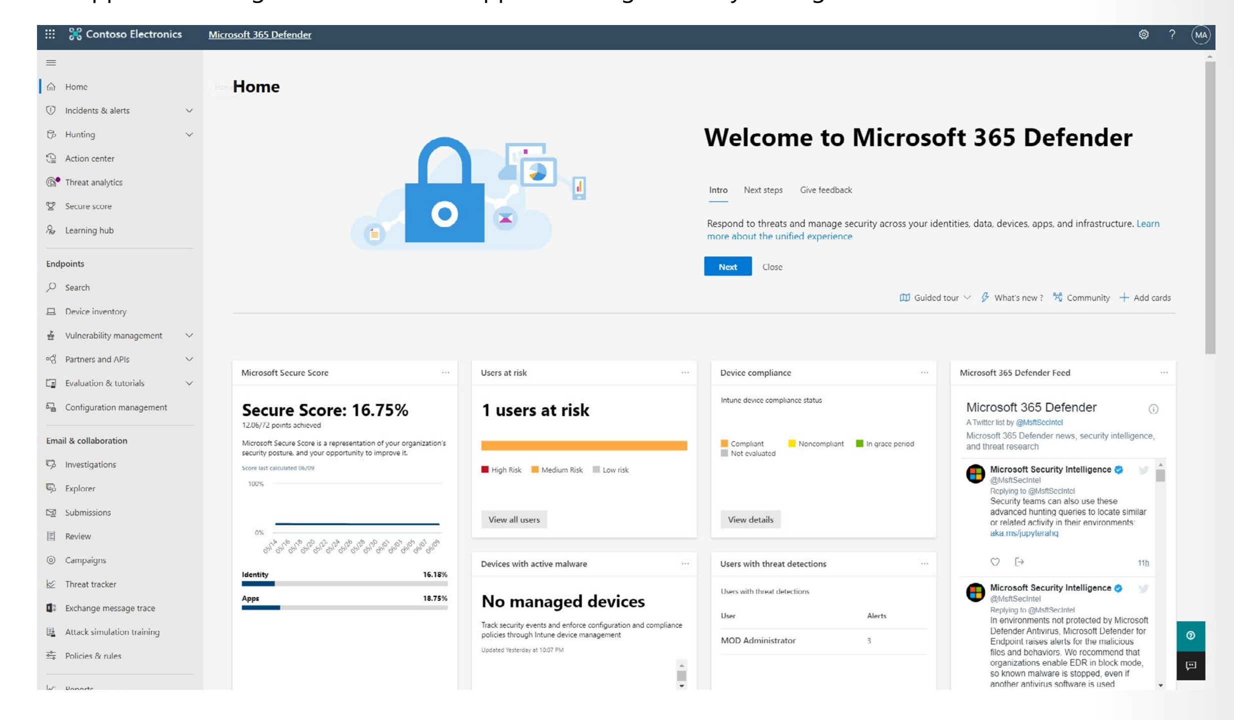
Describe the Microsoft 365 Defender portal

Microsoft 365 Defender natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. The Microsoft 365 Defender portal brings this functionality together into a central place that is designed to meet the needs of security teams and emphasizes quick access to information, simpler layouts. Through the Microsoft 365 Defender portal you can view the security health of your organization.

The Microsoft 365 Defender portal home page shows many of the common cards that security teams need. The composition of cards and data depends on the user role. Because the Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day-to-day jobs.

The cards fall into these categories:

- Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors.
- Data - Help track user activity that could lead to unauthorized data disclosure.
- Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.
- Apps - Gain insight into how cloud apps are being used in your organization.



The Microsoft 365 Defender portal allows admins to tailor the navigation pane to meet daily operational needs. Admins can customize the navigation pane to show or hide functions and services based on their specific preferences. Customization is specific to the individual admin, so other admins won't see these changes.

NOTE: You must be assigned an appropriate role, such as Global Administrator, Security Administrator, Security Operator, or Security Reader in Azure Active Directory to access the Microsoft 365 Defender portal.

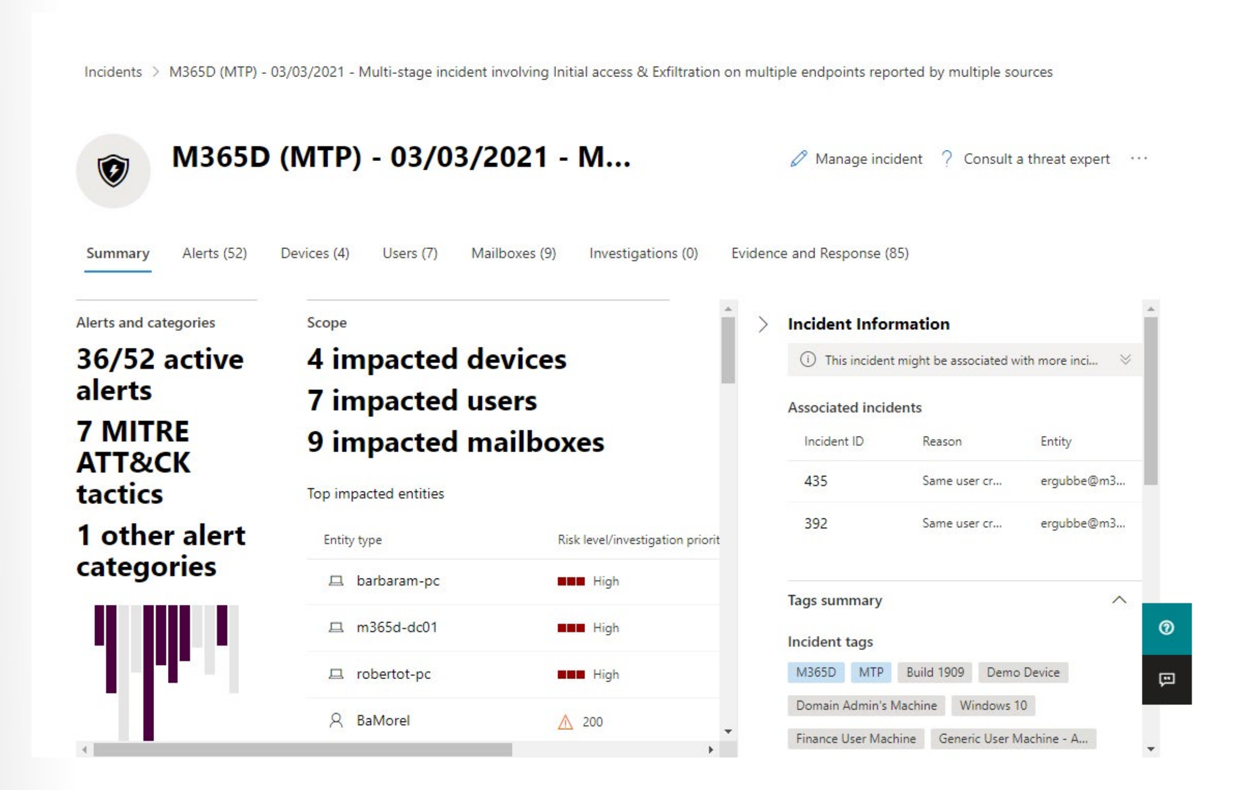
The left navigation pane provides security professionals easy access to the email and collaboration capabilities of Microsoft Defender for Office 365 and the capabilities for Microsoft Defender for Endpoint, which were described in the previous units. Listed below we describe a few of the other capabilities accessible from the left navigation bar in the Microsoft 365 Defender portal.

Incidents and alerts

Microsoft 365 services and apps create alerts when they detect a suspicious or malicious event or activity. Individual alerts provide valuable clues about a completed or ongoing attack. These alerts are automatically aggregated by Microsoft 365 Defender. It's the grouping of these related alerts that form an incident. The incident provides a comprehensive view and context of an attack.

The incidents queue is a central location lists each incident by severity. Selecting an incident name displays a summary of the incident and provides access to tabs with additional information, including:

- All the alerts related to the incident.
- All the users that have been identified to be part of or related to the incident.
- All the mailboxes that have been identified to be part of or related to the incident.
- All the automated investigations triggered by the alerts in the incident.
- All the supported evidence and response.



Hunting

Advanced hunting is a query-based threat-hunting tool that lets security professionals explore up to 30 days of raw data. Advanced hunting queries enable security professionals to proactively search for threats, malware, and malicious activity across your endpoints, Office 365 mailboxes, and more. Threat-hunting queries can be used to build custom detection rules. These rules run automatically to check for and then respond to suspected breach activity, misconfigured machines, and other findings.

Threat analytics

Threat analytics is our in-product threat intelligence solution from expert Microsoft security researchers. It's designed to assist security teams track and respond to emerging threats. The threat analytics dash-board highlights the reports that are most relevant to your organization. It includes the latest threats, high impact threats (threats with the most active alerts affecting your organization), and high exposure threats.

Selecting a specific threat from the dashboard provides a threat analytics report that provides more detailed information that includes detailed analyst report, impacted assets, mitigations, and much more.



Secure Score

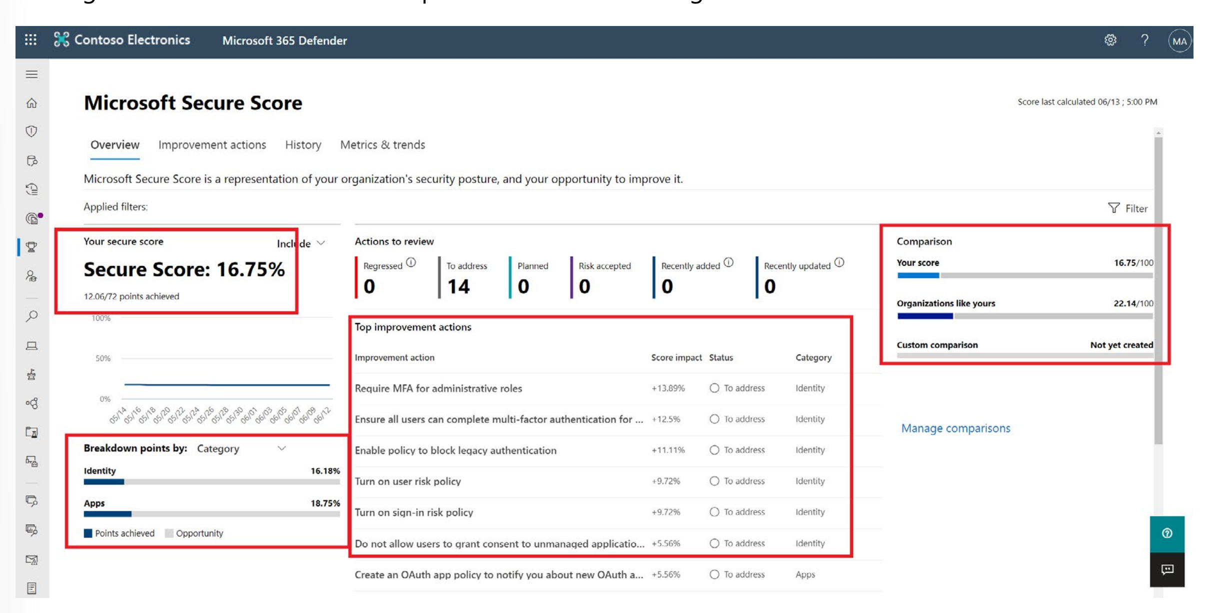
Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture. The higher the score, the better your protection. From a centralized dash-board in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Secure Score helps organizations:

- Report on the current state of their security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Compare benchmarks and establish key performance indicators (KPIs).

Currently Microsoft Secure Score supports recommendations for Microsoft 365 (including Exchange Online), Azure Active Directory, Microsoft Defender for Endpoint, Microsoft Defender for Identity, Micro-soft Defender Cloud Apps, and Microsoft Teams. New recommendations are being added to Secure Score all the time.

The image below shows an organization's Secure Score, a breakdown of the score by points, and the improvement actions that can boost the organization's score. Finally, it provides an indication of how well the organization's Secure Score compares to other similar organizations.



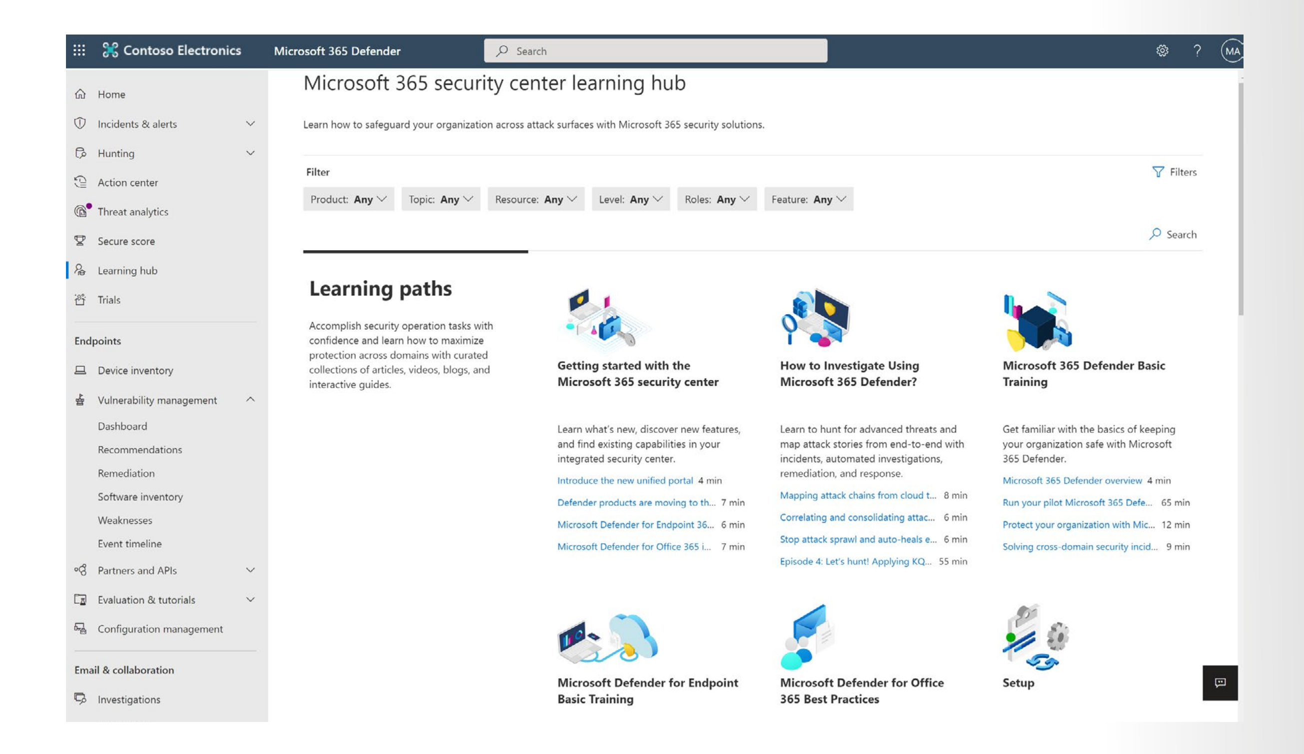
In following interactive click-through you can explore Microsoft Secure Score. Select the link below and follow the prompts on the screen.

Differences between secure score in Microsoft 365 Defender and Microsoft Defender for Cloud

There's a secure score for both Microsoft 365 Defender and Microsoft Defender for Cloud, but they're subtly different. Secure score in Microsoft Defender for Cloud is a measure of the security posture of your Azure subscriptions. Secure score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

Learning hub

The Microsoft 365 Defender portal includes a learning hub that bubbles up official guidance from resources such as the Microsoft security blog, the Microsoft security community on YouTube, and the official documentation at docs.microsoft.com.



Reports

Reports are unified in Microsoft 365 Defender. Admins can start with a general security report, and branch into specific reports about endpoints, email & collaboration. The links here are dynamically generated based upon workload configuration.

Reports

View information about security trends and track the protection status of your identities, data, devices, apps, and infrastructure.

6 items

Name	Description
General (1)	
Security report	View information about security trends and track the protection st...
Endpoints (1)	
Attack surface reduction rules	View information about detections, misconfiguration, and suggest...
Email & collaboration (4)	
Email & collaboration reports	Review Microsoft recommended actions to help improve email an...
Manage schedules	Manage the schedule for the reports security teams use to mitigat...
Reports for download	Download one or more of your reports.
Exchange mail flow reports	Deep link to Exchange mail flow report in the Exchange admin cen...

Permissions & roles

Access to Microsoft 365 Defender is configured with Azure Active Directory global roles or by using custom roles.

Knowledge check

Multiple choice

Item 1. A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft 365 Defender suite is best suited for this purpose?

- ☐ Microsoft Defender for Office 365.
- ☐ Microsoft Defender for Endpoint.
- ☐ Microsoft Defender for Identity.

Multiple choice

Item 2. A cloud access security broker (CASB) provides protection across 4 areas/pillars: visibility to detect all cloud services, data security, threat protection, and compliance. These pillars represent the basis of the Cloud App Security framework upon which Microsoft Defender for Cloud Apps is built. Which pillar is responsible for identifying and controlling sensitive information?

- ☐ Threat protection.
- ☐ Compliance.
- ☐ Data Security.

Multiple choice

Item 3. Which of the following is a cloud-based security solution that identifies, detects, and helps to investigate advanced threats, compromised identities, and malicious insider actions directed at your organization?

- ☐ Microsoft Defender for Office 365
- ☐ Microsoft Defender for Identity
- ☐ Microsoft Defender for Cloud Apps

Multiple choice

Item 4. Admins in the organization are using the Microsoft 365 Defender portal every day. They want to quickly get an understanding of the organization's current security posture. Which capability in the Microsoft 365 Defender portal will they use?

- ☐ Reports.
- ☐ Secure Score.
- ☐ Policies.

Summary and resources

In this lesson, you learned how Microsoft 365 Defender can help protect your organization. You explored each of the different Defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps. You also explored the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, reports, and incident management.

Now that you've completed this lesson, you'll be able to:

- Describe the Microsoft 365 Defender service.
- Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.
- Describe and explore Microsoft 365 Defender portal.

Learn more

To find out more about any of the topics covered in this lesson, visit these links:

- **Microsoft 365 Defender**[25]

25 https://docs.microsoft.com/microsoft-365/security/mtp/microsoft-threat-protection

- **Microsoft Defender for Identity**[26]
- **Microsoft Defender for Office 365**[27]
- **Microsoft Defender for Endpoint**[28]
- **Microsoft Defender for Cloud Apps**[29]
- **Overview of the Microsoft 365 Defender portal**[30]
- **Incident response with Microsoft 365 Defender**[31]
- **Threat analytics in Microsoft 365 Defender**[32]
- **Microsoft Secure Score**[33]
- **Integrated reports**[34]
- **Incidents overview in Microsoft 365 Defender**[35]

26 https://docs.microsoft.com/defender-for-identity/what-is
27 https://docs.microsoft.com/microsoft-365/security/office-365-security/office-365-atp
28 https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection
29 https://docs.microsoft.com/cloud-app-security/what-is-cloud-app-security
30 https://docs.microsoft.com/microsoft-365/security/mtp/overview-security-center?view=o365-worldwide
31 https://docs.microsoft.com/microsoft-365/security/defender/incidents-overview?view=o365-worldwide
32 https://docs.microsoft.com/microsoft-365/security/defender/threat-analytics?view=o365-worldwide
33 https://docs.microsoft.com/microsoft-365/security/mtp/microsoft-secure-score?view=o365-worldwide
34 https://docs.microsoft.com/microsoft-365/security/mtp/overview-security-center?view=o365-worldwide#integrated-reports
35 https://docs.microsoft.com/microsoft-365/security/mtp/incidents-overview?view=o365-worldwide

Answers

Multiple choice

Item 1. The security admin has created an Azure Network Security Group (NSG) to filter network traffic to a virtual machine. The admin wants to allow inbound traffic using the Remote Desktop Protocol (RDP), but the default NSG rules are currently blocking all inbound traffic that is not from another virtual network or an Azure load balancer. What does the security admin have to do to allow inbound traffic using RDP?

☐ Delete the default rule.

■ Create a new network security rule that allows RDP traffic and that has a higher priority than the default rule.

☐ There is nothing the admin can do, RDP traffic is not supported with NSGs.

Explanation
Default NSG rules cannot be deleted, but you can override them by creating new rules with higher priorities.

Multiple choice

Item 2. The security admin wants to protect Azure resources from DDoS attacks, which Azure DDoS Protection tier will the admin use to target Azure Virtual Network resources?

☐ Basic.

■ Standard.

☐ Advanced.

Explanation
The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources.

Multiple choice

Item 3. Your organization has several virtual machines in Azure. The security admin wants to deploy Azure Bastion to get secure access to the virtual machines in Azure. What should the admin keep in mind?

■ Azure Bastion is deployed per virtual network, with support for virtual network peering.

☐ Azure Bastion is deployed per subscription.

☐ Azure Bastion is deployed per virtual machine.

Explanation
Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine.

Multiple choice

Item 4. Much of your organization's application data is in Azure. The security admin wants to take advantage of the encryption capabilities in Azure, which service would the admin use to store the application's secrets?

☐ Transparent data encryption.

☐ Secrets management.

■ Azure Key Vault.

Explanation
Azure Key Vault is a centralized cloud service for storing your application secrets.

Multiple choice

Item 1. An organization is using Azure and wants to improve their security best practices. Which Azure specific benchmark would the IT security team need to consider?

■ Azure Security Benchmark.

□ Center for Internet Security.

□ Microsoft cybersecurity group

Explanation
The Azure Security Benchmark provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure.

Multiple choice

Item 2. Your organization is using Microsoft Defender for Cloud to assess your resources, subscriptions, and organization for security issues. Your organization's overall secure score is low and needs to improve. How would a security admin go about improving the score?

□ Close old security recommendations.

■ Remediate security recommendations.

□ Move security recommendations to resolved.

Explanation
To improve your secure score, remediate security recommendations from your recommendations list.

Multiple choice

Item 3. An organization wants to add vulnerability scanning for its Azure resources to view, investigate, and remediate the findings directly within Microsoft Defender for Cloud. What functionality of Microsoft Defender for Cloud would they need to consider?

□ Secure score and recommendations functionality that is part of the CSPM pillar of Microsoft Defender for Cloud.

■ The enhanced functionality that is provided through the Microsoft Defender plans and is part of the CWP pillar of Microsoft Defender for Cloud.

□ Security Benchmarks.

Explanation
Microsoft Defender plans provide enhanced security features for your workloads, including vulnerability scanning.

Multiple choice

Item 1. As the lead admin, it is important to convince your team to start using Microsoft Sentinel. You've put together a presentation. What are the four security operation areas of Microsoft Sentinel that cover this area?

□ Collect, Detect, Investigate, and Redirect.

■ Collect, Detect, Investigate, and Respond.

□ Collect, Detect, Investigate, and Repair.

Explanation
A SIEM/SOAR solution uses collect, detect, investigate, and respond to identify and protect your organizations network perimeter.

Multiple choice

Item 2. Your estate has many different data sources where data is stored. Which tool should be used with Microsoft Sentinel to quickly gain insights across your data as soon as a data source is connected?

■ Azure Monitor Workbooks.

☐ Playbooks.

☐ Microsoft 365 Defender.

Explanation
Using the Microsoft Sentinel integration with Azure Monitor Workbooks, allows you to monitor data and provides versatility in creating custom workbooks.

Multiple choice

Item 1. A lead admin for an organization is looking to protect against malicious threats posed by email messages, links (URLs), and collaboration tools. Which solution from the Microsoft 365 Defender suite is best suited for this purpose?

■ Microsoft Defender for Office 365.

☐ Microsoft Defender for Endpoint.

☐ Microsoft Defender for Identity.

Explanation
Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Multiple choice

Item 2. A cloud access security broker (CASB) provides protection across 4 areas/pillars: visibility to detect all cloud services, data security, threat protection, and compliance. These pillars represent the basis of the Cloud App Security framework upon which Microsoft Defender for Cloud Apps is built. Which pillar is responsible for identifying and controlling sensitive information?

☐ Threat protection.

☐ Compliance.

■ Data Security.

Explanation
Through the Data Security pillar, you can identify and control sensitive information and respond to classification labels on content.

Multiple choice

Item 3. Which of the following is a cloud-based security solution that identifies, detects, and helps to investigate advanced threats, compromised identities, and malicious insider actions directed at your organization?

- ☐ Microsoft Defender for Office 365
- ■ Microsoft Defender for Identity
- ☐ Microsoft Defender for Cloud Apps

Explanation
Microsoft Defender for Identity is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Multiple choice

Item 4. Admins in the organization are using the Microsoft 365 Defender portal every day. They want to quickly get an understanding of the organization's current security posture. Which capability in the Microsoft 365 Defender portal will they use?

- ☐ Reports.
- ■ Secure Score.
- ☐ Policies.

Explanation
Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture.

Module 4 Describe the capabilities of Microsoft compliance solutions

Describe the Service Trust Portal and Privacy with Microsoft

Introduction

Microsoft Cloud services are built on a foundation of trust, security, and compliance. The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices.

In this lesson you'll learn about the Service Trust Portal and resources it provides, including audit reports, security assessments, and compliance guides that enable organizations to manage compliance. You'll learn about Microsoft's commitment to privacy and its privacy principles. Lastly, you'll learn about Microsoft Priva, which helps organizations meet their privacy goals.

After completing this lesson, you'll be able to:

- Describe the offerings of the Service Trust Portal
- Describe Microsoft's privacy principles.
- Describe Microsoft Priva.

Explore the Service Trust Portal

The Service Trust Portal provides information, tools, and other resources about Microsoft security, privacy, and compliance practices. Sign in with your Microsoft cloud services account to access all the available documentation.

From the main menu, you access:



- **Service Trust Portal** – This link provides a quick way to get back to the home page for the Service Trust Portal.
- **Compliance Manager** – This link currently directs users to Compliance Manager in the Microsoft Purview compliance portal. Users are encouraged to use the Microsoft Purview compliance portal for access to Compliance Manager and other compliance management capabilities in Microsoft 365. To find out more, see the Microsoft Compliance Manager documentation in the Learn More section of the Summary and resources unit.
- **Trust Documents** – Trust Documents provides a wealth of security implementation and design information with the goal of making it easier for organizations to meet regulatory compliance objectives, by understanding how Microsoft Cloud services keep customer data secure. To review content, select one of the following options on the Trust Documents pull-down menu.
  - **Audit Reports** provides a list of independent audit and assessment reports on Microsoft's Cloud services is displayed. These reports provide information about Microsoft Cloud services compliance with data protection standards and regulatory requirements.
  - **Data Protection** contains a wealth of resources such as audited controls, white papers, FAQs, penetration tests, risk assessment tools, and compliance guides.
  - **Azure Stack** contains documents that provide security and compliance solutions and support, tailored to the needs of Azure Stack customers.
- **Industries & Regions** – This link provides access to compliance information about Microsoft Cloud services organized by industry and region.
  - **Industry Solutions** directs users to the landing page for the Financial Services industry. This contains information such as compliance offerings, FAQs, and success stories. Resources for more industries will be released in the future, however you can find resources for more industries by going to the Trust Documents > Data Protection page in the STP.
  - **Regional Solutions** provides documents on Microsoft Cloud services compliance with the laws of various countries/regions. Specific countries/regions include Australia, Canada, Czech Republic, Denmark, Germany, Poland, Romania, Spain, and the United Kingdom. links currently have information for: Australia, Canada, Czech Republic, Denmark, Germany, Poland, Romania, Spain, and the United Kingdom.
- **Trust Center** – The option links to the Microsoft Trust Center, which provides more information about privacy, security, and compliance in the Microsoft Cloud.
- **Resources** – This option provides links to Security & Compliance for Office 365, the Microsoft Global Datacenters, and Frequently Asked Questions.
- **My Library** – This feature lets you save documents so that you can quickly access them on your My Library page. You can also set up notifications so that Microsoft sends you an email message when documents in your My Library are updated.
- **More** - This option provides a selection for settings and user privacy settings which are available only to Global Administrators and relate to options associated with Compliance Manager. Admins, however, are encouraged to use the Microsoft Purview compliance portal.

Interactive guide

Explore the Service Trust Portal through an interactive click-through guide. Select the link below to get started and follow the prompts on the screen.

NOTE: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the interactive guide may not reflect the most recent updates.

Explore the Service Trust Portal[1]

Describe Microsoft's privacy principles

Microsoft's products and services run on trust. At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it's used. We empower and defend the privacy choices of every person who uses our products and services.

Microsoft's approach to privacy is built on the following six principles:

- **Control**: Putting you, the customer, in control of your data and your privacy with easy-to-use tools and clear choices. Your data is your business, and you can access, modify, or delete it at any time. Microsoft will not use your data without your agreement, and when we have your agreement, we use your data to provide only the services you have chosen. Your control over your data is reinforced by Microsoft compliance with broadly applicable privacy laws and privacy standards.
- **Transparency**: Being transparent about data collection and use so that everyone can make informed decisions. We only process your data based on your agreement and in accordance with the strict policies and procedures that we've contractually agreed to. When we deploy subcontractors or subprocessors to perform work that requires access to your data, they can perform only the functions that Microsoft has hired them to provide, and they're bound by the same contractual privacy commitments that Microsoft makes to you. The Microsoft Online Services Subprocessor List identifies authorized, subprocessors, who have been audited against a stringent set of security and privacy requirements in advance. This document is available as one of the data protection resources in the Service Trust Portal.
- **Security**: Protecting the data that's entrusted to Microsoft by using strong security and encryption. With state-of-the-art encryption, Microsoft protects your data both at rest and in transit. Our encryption protocols erect barriers against unauthorized access to the data, including two or more independent encryption layers to protect against compromises of any one layer. All Microsoft-managed encryption keys are properly secured and offer the use of technologies such as Azure Key Vault to help you control access to passwords, encryption keys, and other secrets.
- **Strong legal protections**: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right. Microsoft defends your data through clearly defined and well-established response policies and processes, strong contractual commitments, and if necessary, the courts. We believe all government requests for your data should be directed to you. We don't give any government direct or unfettered access to customer data. We will not disclose data to a government or law enforcement agency, except as you direct or where required by law. Microsoft scrutinizes all government demands to ensure they're legally valid and appropriate. If Microsoft receives a request for your data, we'll promptly notify you and provide a copy of the request unless legally prohibited from doing so. Moreover, we'll direct the requesting party to seek the data directly from you. Our contractual commitments to our enterprise and public sector customers include defending your data, which

1 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/LP04M01-Explore-the-Service-Trust-Portal/index.html?azure-portal=true

builds on our existing protections. We'll challenge every government request for commercial and public sector customer data where we can lawfully do so.

- **No content-based targeting**: Not using email, chat, files, or other personal content to target advertising. We do not share your data with advertiser-supported services, nor do we mine it for any purposes like marketing research or advertising.
- **Benefits to you**: When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better. For example:

  - Troubleshooting: Troubleshooting for preventing, detecting, and repairing problems affecting operations of services.
  - Feature improvement: Ongoing improvement of features including increasing reliability and protection of services and data.
  - Personalized customer experience: Data is used to provide personalized improvements and better customer experiences.

These principles form Microsoft's privacy foundation, and they shape the way Microsoft products and services are designed.

Describe Microsoft Priva

Privacy is top of mind for organizations and consumers today, and concerns about how private data is handled are steadily increasing. Regulations and laws impact people around the world, setting rules for how organizations store personal data and giving people rights to manage personal data collected by an organization.

To meet regulatory requirements and build customer trust, organizations need to take a "privacy by default" stance. Rather than manual processes and a patchwork of tools, organizations need a comprehensive solution to address common challenges such as:

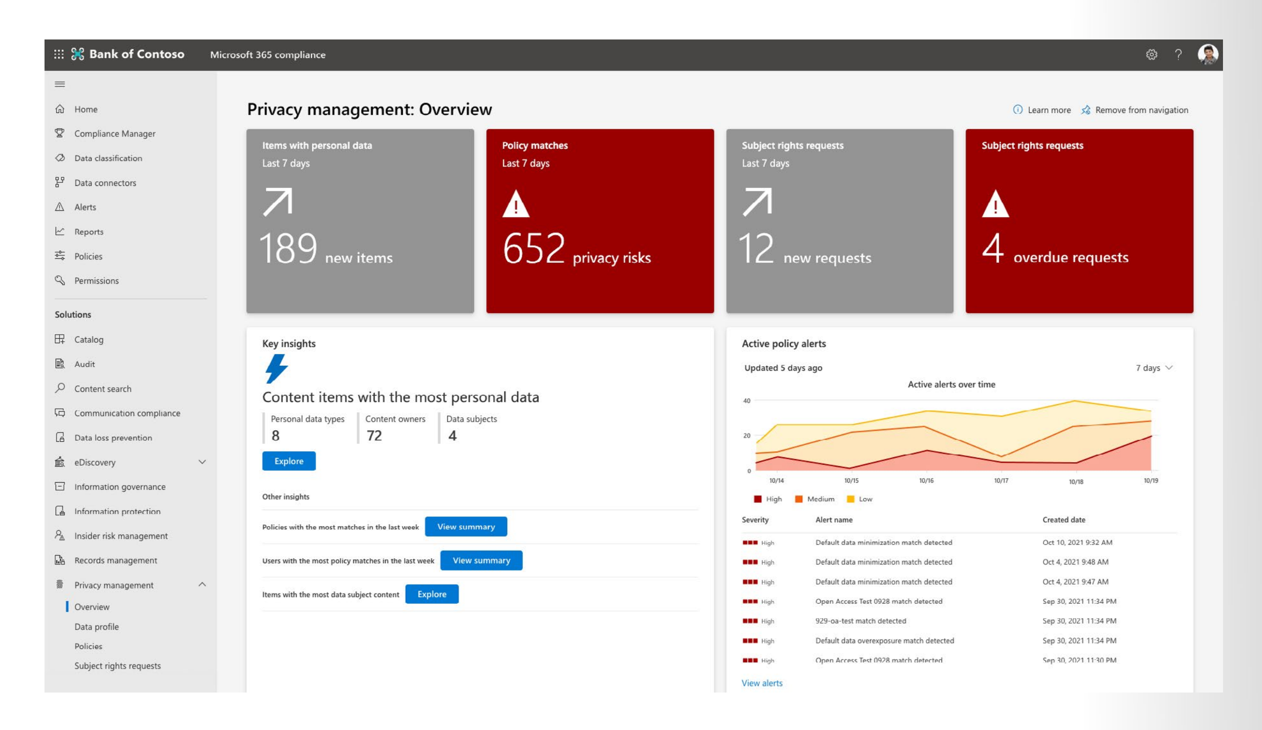
- Helping employees adopt sound data handling practices and training them to spot and fix issues
- Understanding the potential risks in the amount and type of personal data they store and share
- Fulfilling data subject requests, or subject rights requests, efficiently and on-time

Microsoft Priva helps you meet these challenges so you can achieve your privacy goals. Priva's capabilities are available through two solutions: **Priva Privacy Risk Management**, which provides visibility into your organization's data and policy templates for reducing risks; and **Priva Subject Rights Requests**, which provides automation and workflow tools for fulfilling data requests.

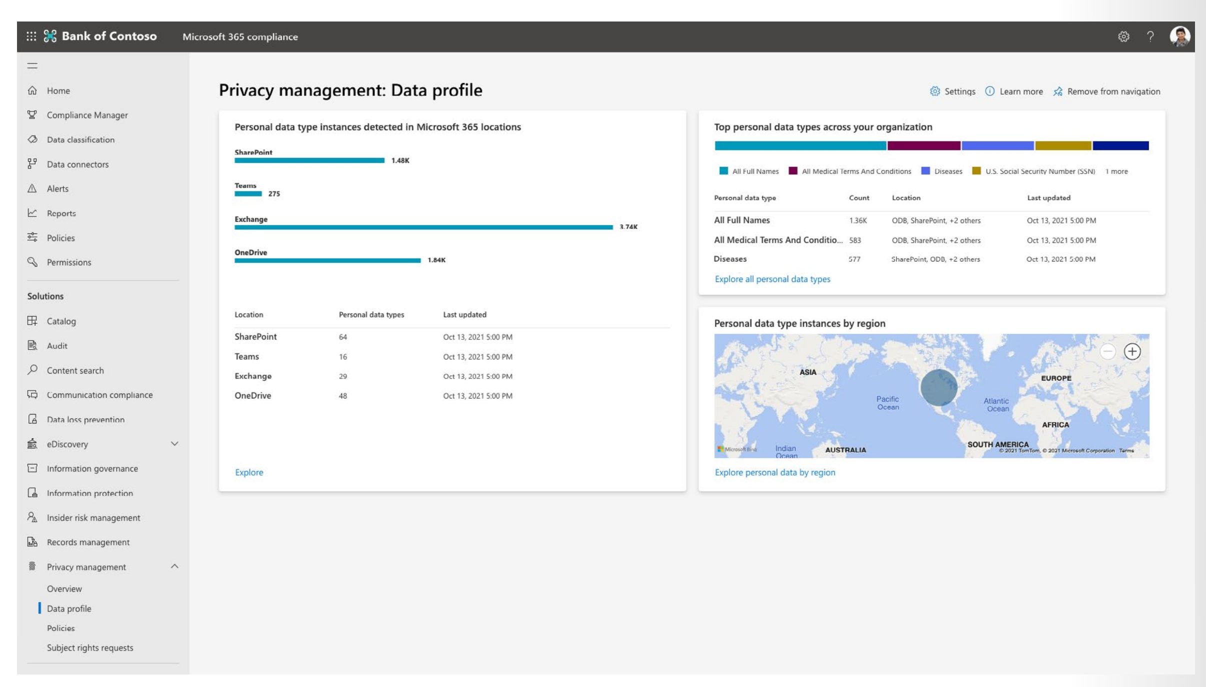
Priva Privacy Risk Management

Microsoft Priva helps you understand the data your organization stores by automating discovery of personal data assets and providing visualizations of essential information. These visualizations can be found on the overview and data profile pages, currently accessible through the Microsoft Purview compliance portal.

The overview dashboard provides an overall view into your organization's data in Microsoft 365. Privacy administrators can monitor trends and activities, identify and investigate potential risks involving personal data, and springboard into key activities like policy management or subject rights request actions.



The data profile page in Priva provides a snapshot view of the personal data your organization stores in Microsoft 365 and where it lives. It also gives insight into the types of data you store.



Priva evaluates your organization's data stored in the following Microsoft 365 services within your Microsoft 365 tenant:

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams

Privacy Risk Management in Microsoft Priva also gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:

- Detect overexposed personal data so that users can secure it.
- Spot and limit transfers of personal data across departments or regional borders.
- Help users identify and reduce the amount of unused personal data that you store.

Priva Subject Rights Requests

In accordance with certain privacy regulations around the world, individuals (or data subjects) may make requests to review or manage the personal data about themselves that companies have collected. These requests are sometimes also referred to as data subject requests (DSRs), data subject access requests (DSARs), or consumer rights requests. For companies that store large amounts of information, finding the relevant data can be a formidable task.

Microsoft Priva can help you handle these inquiries through the Subject Rights Requests solution. It provides workflow, automation, and collaboration capabilities for helping you search for subject data, review your findings, collect the appropriate files, and produce reports.

Knowledge check

Multiple choice

Item 1. When browsing Microsoft compliance documentation in the Service Trust Portal, you have found several documents that are specific to your industry. What is the best way of ensuring you keep up to date with the latest updates?

☐ Save the documents to your My Library.

☐ Print each document so you can easily refer to them.

☐ Download each document.

Multiple choice

Item 2. Microsoft's approach to privacy is built on six principles: Three of the principles are strong legal protections for privacy, no content-based targeting, and benefits to customers from any data we collect. Identify the three other principles that are part of Microsoft's approach to privacy.

☐ Customer control, transparency, and security.

☐ Shared responsibility, transparency, and security.

☐ Customer control, transparency, and zero trust.

Multiple choice

Item 3. Which solution in Microsoft Priva provides visibility into your organization's data and policy templates for reducing risks?

- ☐ Privacy Risk Management.
- ☐ Subject Rights Request.
- ☐ Compliance score.

Summary and resources

In this lesson, you learned about the Microsoft Service Trust Portal and the variety of content resources it provides about Microsoft security, privacy, and compliance practices. You also learned about Microsoft's commitment to privacy and its privacy principles. Lastly, you learned about Microsoft Priva and how it helps organization's meet their privacy goals.

Now that you've completed this lesson, you should be able to:

- Describe the offerings of the Service Trust Portal
- Describe Microsoft's privacy principles.
- Describe Microsoft Priva.

Learn more

To find out more about any of the topics covered in this lesson, visit these links:

- **Service Trust Portal**[2]
- **Get started with the Microsoft Service Trust Portal**[3]
- **Trust Center**[4]
- **Privacy overview**[5]
- **Privacy at Microsoft**[6]
- **Microsoft Privacy Statement**[7]
- **Microsoft Privacy**[8]
- **Learn about Microsoft Priva**[9]

2 https://servicetrust.microsoft.com/
3 https://docs.microsoft.com/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide
4 https://www.microsoft.com/trust-center
5 https://docs.microsoft.com/compliance/assurance/assurance-privacy
6 https://privacy.microsoft.com/
7 https://privacy.microsoft.com/privacystatement
8 https://docs.microsoft.com/privacy/
9 https://docs.microsoft.com/privacy/priva/priva-overview

Describe the compliance management capabilities of Microsoft Purview

Introduction

Organizations must stay in line with compliance-related legal, regulatory, and privacy standards to protect their customers, partners, and themselves. Microsoft Purview provides tools and capabilities to enable organizations to manage compliance.

The Microsoft Purview compliance portal is the portal for organizations to manage their compliance needs using integrated solutions for information protection, information governance, insider risk management, auditing, and more.

In this lesson, you'll learn about the Microsoft Purview compliance portal. You'll learn about Compliance Manager and compliance score, which can help organizations manage, simplify, and improve compliance across their organization.

After completing this lesson, you'll be able to:

- Describe the Microsoft Purview compliance portal.
- Describe Compliance Manager.
- Describe the use and benefits of compliance score.

Describe the Microsoft Purview compliance portal

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. The Microsoft 365 compliance center is now the Microsoft Purview Compliance portal. For more information about Microsoft Purview, see the **blog announcement**[10]

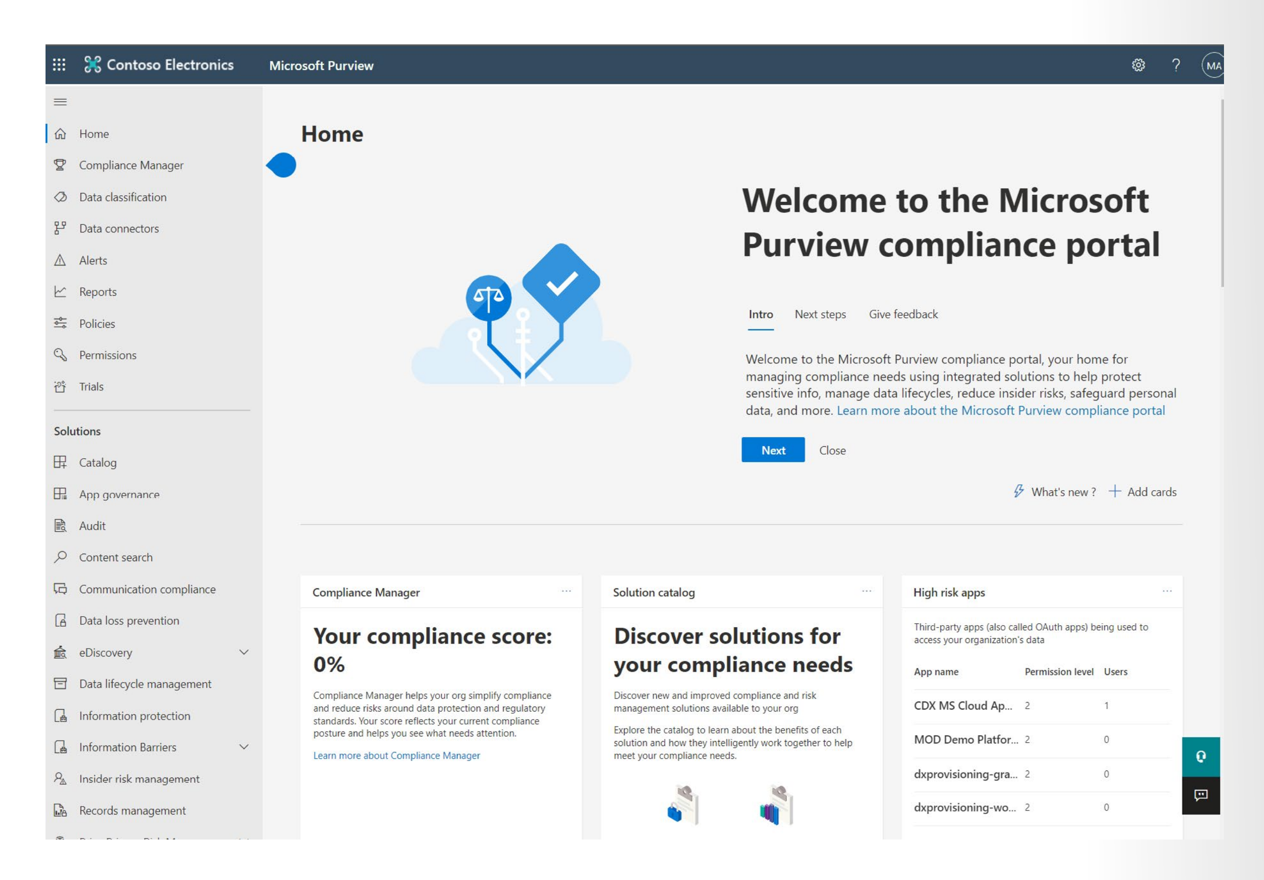
The Microsoft Purview compliance portal brings together all of the tools and data that are needed to help understand and manage an organization's compliance needs.

The compliance portal is available to customers with a Microsoft 365 SKU with one of the following roles:

- Global administrator
- Compliance administrator
- Compliance data administrator

When an admin signs in to the Microsoft Purview compliance portal, the card section on the home page shows, at a glance, how your organization is doing with data compliance, what solutions are available for your organization, and a summary of any active alerts. Admins can customize the card section by moving cards around or adding/removing cards that are displayed on the home screen.

10 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

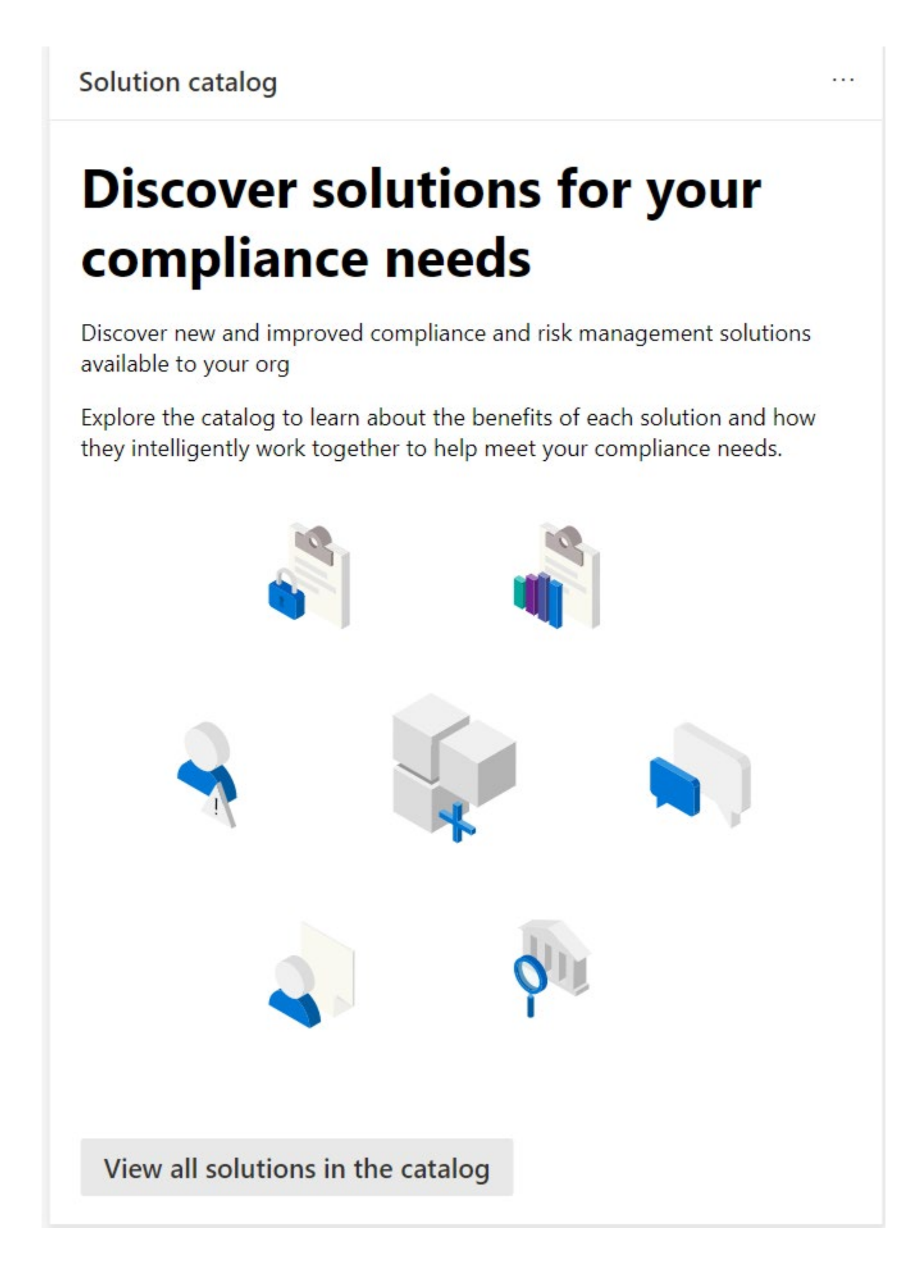


The default compliance portal home page contains several cards including:

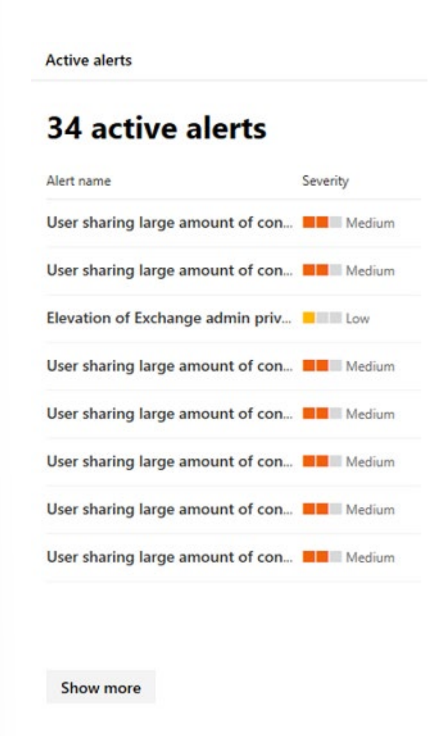
- The **Compliance Manager** card. This card leads you to the Microsoft Purview Compliance Manager solution. Compliance Manager helps simplify the way you manage compliance. It calculates a risk-based compliance score that measures progress toward completing recommended actions to reduce risks associated with data protection and regulatory standards. The Compliance Manager solution also provides workflow capabilities and built-in control mapping to help you efficiently carry out improvement actions.



- The **Solution catalog** card, links to collections of integrated solutions to help you manage end-to-end compliance scenarios. Solutions areas included:
  - **Information protection & governance**. These solutions help organizations classify, protect, and retain your data where it lives and wherever it goes. Included are data lifecycle management, data loss prevention, information protection, and records management.
  - **Privacy**. Build a more privacy-resilient workplace. Privacy management gives actionable insights on your organization's personal data to help you spot issues and reduce risks.
  - **Insider risk management**. These solutions help organizations identify, analyze, and remediate internal risks before they cause harm. Included are communication compliance, information barriers, and insider risk management.
  - **Discovery & respond**. These solutions help organizations quickly find, investigate, and respond with relevant data. Included are Audit, data subject requests, and eDiscovery.

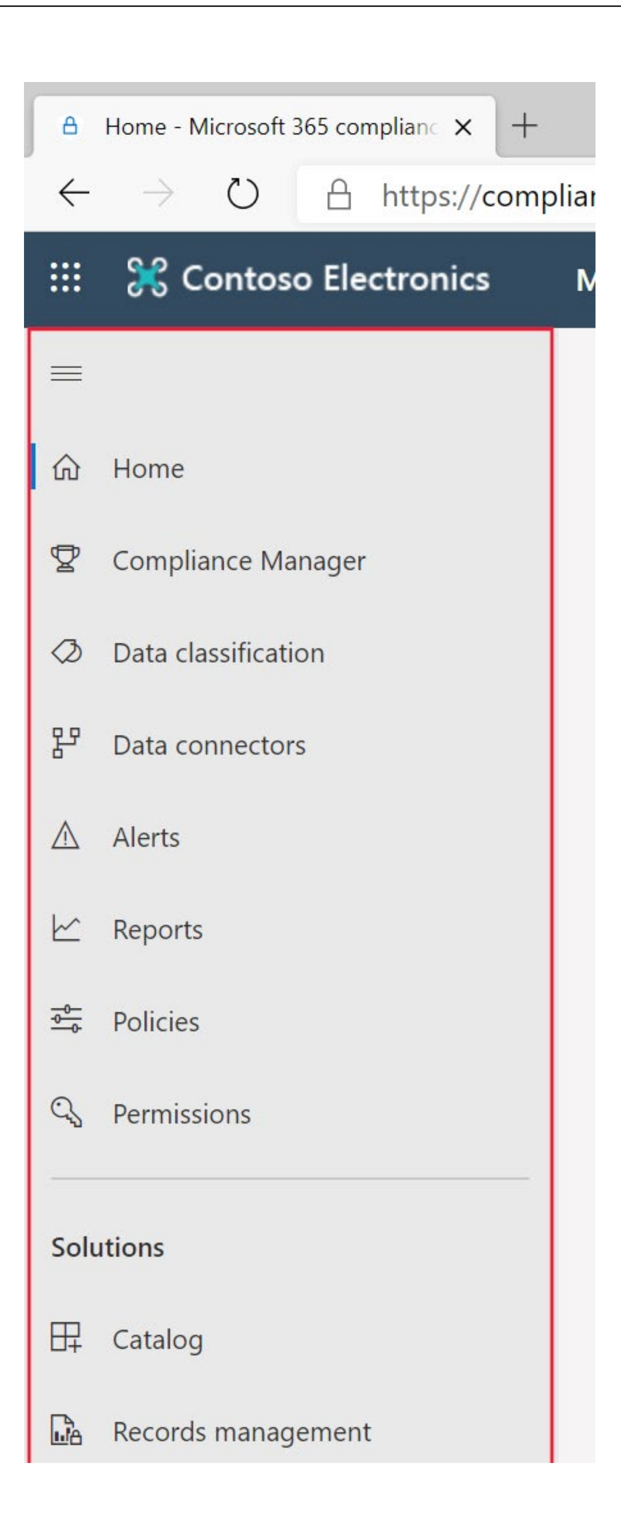


- The **Active alerts** card includes a summary of the most active alerts and a link where admins can view more detailed information, such as alert severity, status, category, and more.



Navigation

In addition to the cards on the home page, there’s a navigation pane on the left of the screen that gives easy access to the Compliance Manager and the Data Classification page where you can get snapshots of how sensitive information and labels are being used across your organization's locations. You can access alerts, reports, policies, and all the solutions that are included in the solutions catalog. There's access to data connectors that you can use to import non-Microsoft data to Microsoft 365 so it can be covered by your compliance solutions. The **Customize navigation** control allows customization of which items appear in the navigation pane.



Interactive guide

In this interactive guide, you'll explore some of the capabilities of the Microsoft Purview compliance portal, your home for managing compliance needs using integrated solutions for information protection, information governance, insider risk management, discovery, and more. Select the link below to get started.

NOTE: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the interactive guide may not reflect the most recent updates.

Interactive guide - Explore the compliance portal[11]

Describe Compliance Manager

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft Compliance Manager is now Microsoft Purview Compliance Manager. For more information about Microsoft Purview, see the **blog announcement**[12]

Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps admins to manage an organization's compliance requirements with greater ease and convenience. Compliance Manager can help organizations throughout their compliance journey, from taking inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

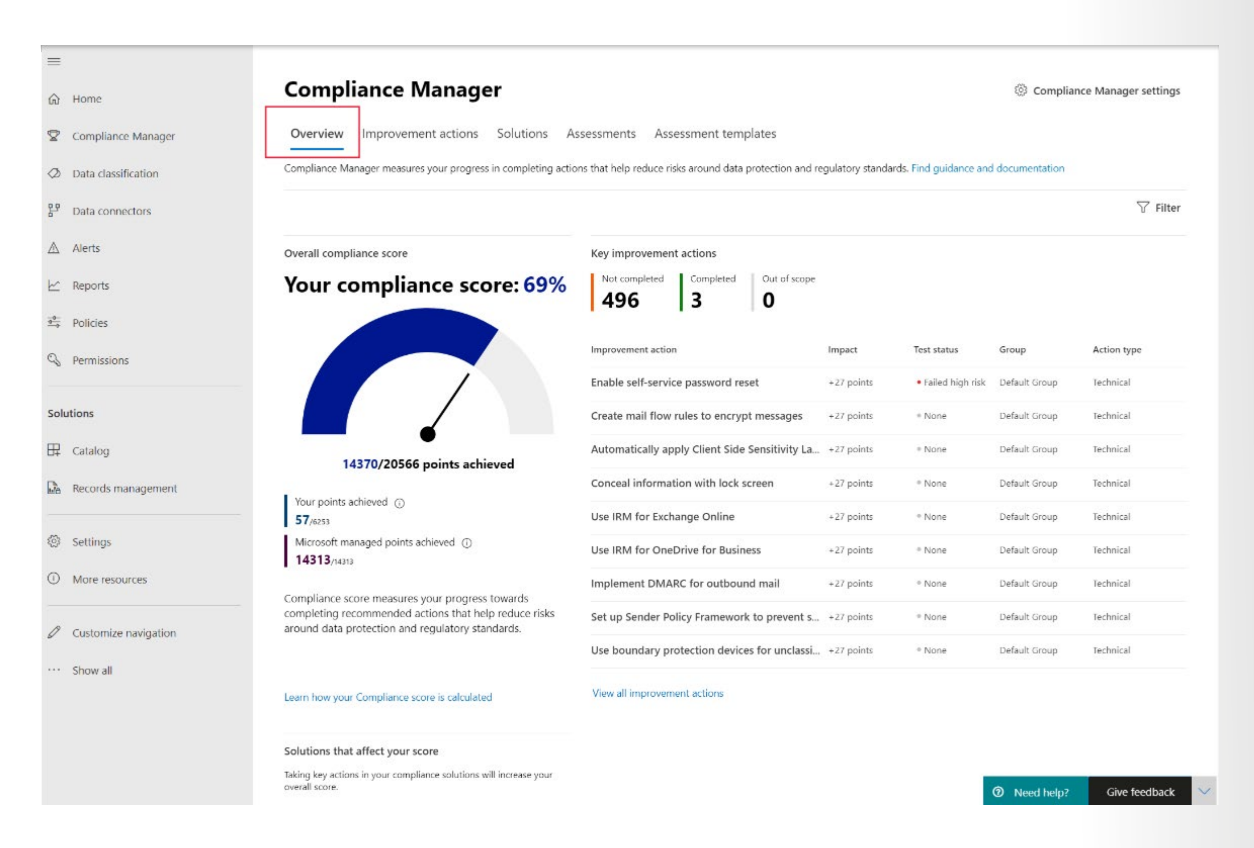
Compliance Manager - video[13], provides a quick overview of Compliance Manager. **NOTE**: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the video may not reflect the most recent updates.

Compliance Manager helps simplify compliance and reduce risk by providing:

- Prebuilt assessments based on common regional and industry regulations and standards. Admins can also use custom assessment to help with compliance needs unique to the organization.
- Workflow capabilities that enable admins to efficiently complete risk assessments for the organization.
- Step-by-step improvement actions that admins can take to help meet regulations and standards relevant to the organization. Some actions will also be managed for the organization by Microsoft. Admins will get implementation details and audit results for those actions.
- Compliance score, which is a calculation that helps an organization understand its overall compliance posture by measuring how it's progressing with improvement actions.

The Compliance Manager dashboard shows the current compliance score, helps admins to see what needs attention, and guides them to key improvement actions.

11 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/explore-the-compliance-portal/index.html?azure-portal=true
12 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/
13 https://www.microsoft.com/videoplayer/embed/RE4FGYZ



Compliance Manager uses several data elements to help manage compliance activities. As admins use Compliance Manager to assign, test, and monitor compliance activities, it's helpful to have a basic understanding of the key elements: controls, assessments, templates, and improvement actions.

Controls

A control is a requirement of a regulation, standard, or policy. It defines how to assess and manage system configuration, organizational process, and people responsible for meeting a specific requirement of a regulation, standard, or policy.

Compliance Manager tracks the following types of controls:

- **Microsoft-managed controls**: controls for Microsoft cloud services, which Microsoft is responsible for implementing.
- **Your controls**: sometimes referred to as customer-managed controls, these are implemented and managed by the organization.
- **Shared controls**: responsibility for implementing these controls is shared by the organization and Microsoft.

Compliance Manager continuously assesses controls by scanning through your Microsoft 365 environment and detecting your system settings, continuously and automatically updating your technical action status.

Assessments

An assessment is a grouping of controls from a specific regulation, standard, or policy. Completing the actions within an assessment helps to meet the requirements of a standard, regulation, or law. For

example, an organization may have an assessment that, when completed, helps to bring the organization's Microsoft 365 settings in line with ISO 27001 requirements.

An assessment consists of several components including the services that are in-scope, the controls, and an assessment score that shows progress towards completing the actions needed for compliance.

Templates

Compliance Manager provides templates to help admins to quickly create assessments. They can modify these templates to create an assessment optimized for their needs. Admins can also build a custom assessment by creating a template with their own controls and actions. For example, the admin may want a template to cover an internal business process control, or a regional data protection standard that isn't covered by one of Microsoft's 150-plus prebuilt assessment templates.

Improvement actions

Improvement actions help centralize compliance activities. Each improvement action provides recommended guidance that's intended to help organizations to align with data protection regulations and standards. Improvement actions can be assigned to users in the organization to do implementation and testing work. Admins can also store documentation, notes, and record status updates within the improvement action.

Benefits of Compliance Manager

Compliance Manager provides many benefits, including:

- Translating complicated regulations, standards, company policies, or other control frameworks into a simple language.
- Providing access to a large variety of out-of-the-box assessments and custom assessments to help organizations with their unique compliance needs.
- Mapping regulatory controls against recommended improvement actions.
- Providing step-by-step guidance on how to implement the solutions to meet regulatory requirements.
- Helping admins and users to prioritize actions that will have the highest impact on their organizational compliance by associating a score with each action.

Interactive guide

In this interactive guide, you'll explore Compliance Manager. Select the link below to get started and follow the prompts on the screen.

NOTE: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the interactive guide may not reflect the most recent updates.

Interactive guide - Explore Compliance Manager.[14]

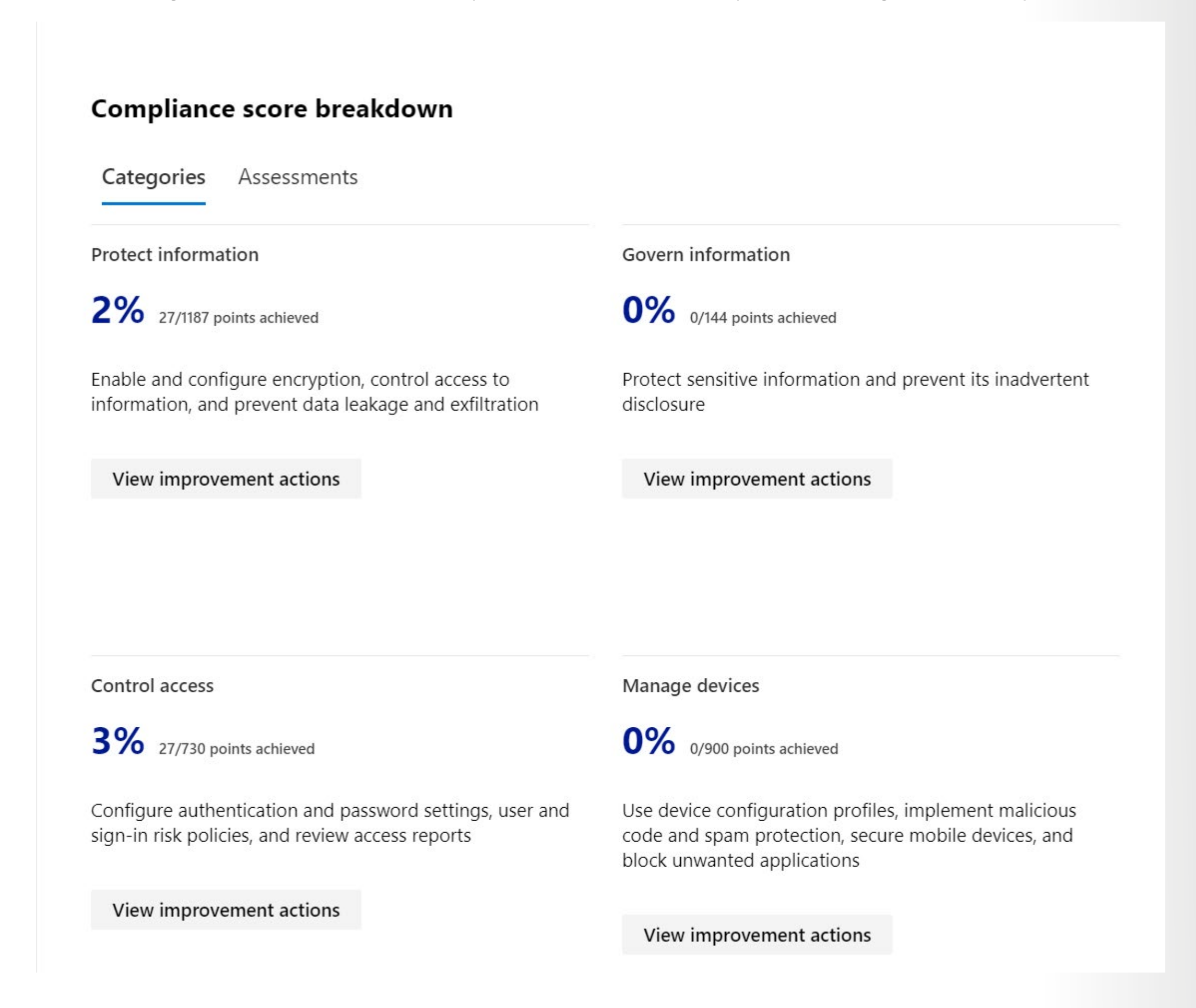
14 https://edxinteractivepage.blob.core.windows.net/edxpages/sc-900/explore-compliance-manager/index.html?azure-portal=true

Describe compliance score

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft Compliance Manager is now Microsoft Purview Compliance Manager. For more information about Microsoft Purview, see the **blog announcement**[15]

Compliance score measures progress in completing recommended improvement actions within controls. The score can help an organization to understand its current compliance posture. It also helps organizations to prioritize actions based on their potential to reduce risk.

Admins can get a breakdown of the compliance score in the Compliance Manager overview pane.



How to understand the compliance score

The overall compliance score is calculated using scores that are assigned to actions. Actions come in two types:

- **Your improved actions**: actions that the organization is expected to manage.
- **Microsoft actions**: actions that Microsoft manages for the organization.

15 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

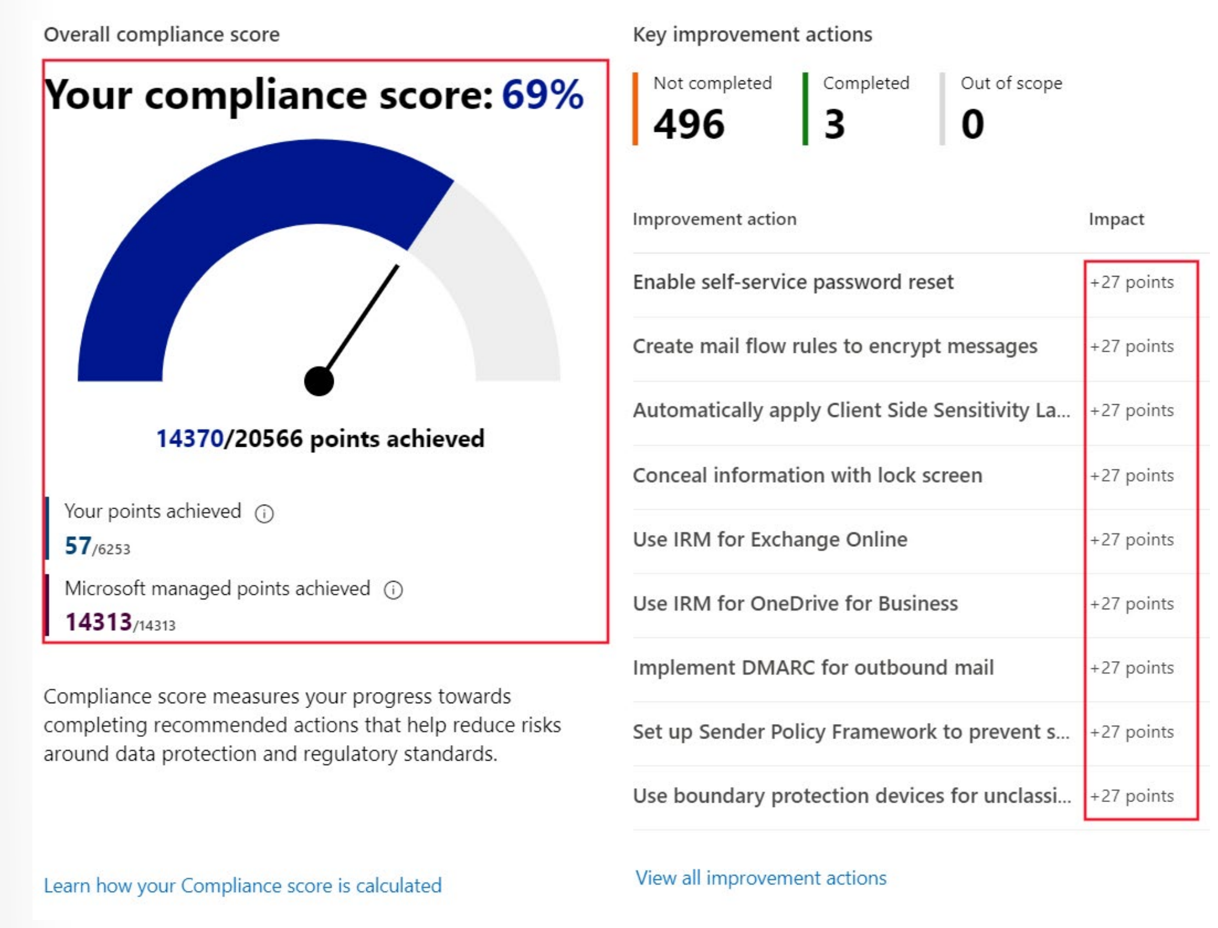
Actions are categorized as mandatory, discretionary, preventative, detective, or corrective:

- **Mandatory** – these actions shouldn't be bypassed. For example, creating a policy to set requirements for password length or expiration.
- **Discretionary** – these actions depend on the users understanding and adhering to a policy. For example, a policy where users are required to ensure their devices are locked before they leave them.

The following are subcategories of actions that can be classified as mandatory or discretionary:

- **Preventative** actions are designed to handle specific risks, like using encryption to protect data at rest if there were breaches or attacks.
- **Detective** actions actively monitor systems to identify irregularities that could represent risks, or that can be used to detect breaches or intrusions. Examples of these types of actions are system access audits, or regulatory compliance audits.
- **Corrective** actions help admins to minimize the adverse effects of security incidents, by undertaking corrective measures to reduce their immediate effect or possibly even reverse damage.

Organizations accumulate points for every action completed. And the compliance score is shown as a percentage representing all the actions completed, compared with the ones outstanding.



What is the difference between Compliance Manager and compliance score?

Compliance Manager is an end-to-end solution in the Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization. The compliance score is available through Compliance Manager.

Compliance Manager gives admins the capabilities to understand and increase their compliance score, so they can ultimately improve the organization's compliance posture and help it to stay in line with compliance requirements.

Knowledge check

Multiple choice

Item 1. A new admin has joined the team and needs to be able to access the Microsoft Purview compliance portal. Which of the following roles could the admin use to access the compliance portal?

- ☐ Compliance Administrator role
- ☐ Helpdesk Administrator role
- ☐ User Administrator role

Multiple choice

Item 2. Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

- ☐ Controls that both external regulators and Microsoft share responsibility for implementing.
- ☐ Controls that both your organization and external regulators share responsibility for implementing.
- ☐ Controls that both your organization and Microsoft share responsibility for implementing.

Multiple choice

Item 3. A customer has requested a presentation on how the Microsoft Purview compliance portal can help improve their organization's compliance posture. The presentation will need to cover Compliance Manager and compliance score. What is the difference between Compliance Manager and compliance score?

- ☐ Compliance Manager is an end-to-end solution in the Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.
- ☐ Compliance Manager is an end-to-end solution in Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a score the organization receives from regulators for successful compliance.
- ☐ Compliance Manager is the regulator who will manage your compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

Summary and resources

You've learned about the various tools provided by Microsoft Purview to manage compliance for your organization. You explored the compliance portal, which enables organizations to manage their compliance needs. You learned how Compliance Manager and compliance score can help organizations manage, simplify, and improve compliance across their organization.

Now that you've completed this lesson, you'll be able to:

- Describe the Microsoft Purview compliance portal.
- Describe Compliance Manager.
- Describe the use and benefits of compliance score.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Microsoft Purview compliance portal**[16]
- **Microsoft Purview Compliance Manager**[17]
- **Compliance score calculation**[18]
- **Compliance Manager frequently asked questions**[19]

16 https://docs.microsoft.com/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide
17 https://docs.microsoft.com/microsoft-365/compliance/compliance-score?view=o365-worldwide#relationship-to-compliance-manager
18 https://docs.microsoft.com/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide
19 https://docs.microsoft.com/microsoft-365/compliance/compliance-score-faq?view=o365-worldwide#what-is-the-difference-between-compliance-score-and-compliance-manager

Describe information protection and data life-cycle management in Microsoft Purview

Introduction

Organizations need to protect all sorts of information, including financial and personal information. This must be done to ensure customers, employees, and the organization are protected from risks. The organization needs to stay in line with compliance standards wherever it operates.

Information protection and data lifecycle management in Microsoft Purview helps organizations classify, protect, and retain their data where it lives and wherever it goes.

In this lesson, you'll learn about how Microsoft Purview solutions like data classification, records management, and data loss prevention, can help organizations with their information protection and data lifecycle management needs.

After completing this lesson, you'll be able to:

- Describe data classification capabilities.
- Describe data loss prevention.
- Describe records management.

Know your data, protect your data, and govern your data

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft Information Protection is now Microsoft Purview Information Protection. Microsoft Information Governance is now Microsoft Purview Data Lifecycle Management. For more information about Microsoft Purview, see the **blog announcement**[20]

Microsoft Purview Information Protection discovers, classifies, and protects sensitive and business-critical content throughout its lifecycle across your organization. It provides the tools to know your data, protect your data, and prevent data loss.

Microsoft Purview Data Lifecycle Management manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't. It gives organizations the capabilities to govern their data, for compliance or regulatory requirements.

Information protection and data lifecycle management work together to classify, protect, and govern your data where it lives, and wherever it goes.

20 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/



- **Know your data**: Organizations can understand their data landscape and identify important data across on-premises, cloud, and hybrid environments. Capabilities and tools such as trainable classifiers, activity explorer, and content explorer allow organizations to know their data.
- **Protect your data**: Organizations can apply flexible protection actions including encryption, access restrictions, and visual markings.
- **Prevent data loss**: Organizations can detect risky behavior and prevent accidental oversharing of sensitive information. Capabilities such as data loss prevention policies and endpoint data loss prevention enable organizations to avoid data loss.
- **Govern your data**: Organizations can automatically keep, delete, and store data and records in a compliant manner. Data lifecycle management capabilities, like retention policies, retention labels, and records management enable organizations to govern their data.

Describe the data classification capabilities of the compliance portal

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. For more information about Microsoft Purview, see the **blog announcement**[21]

Organizations need to know their data to identify important information across the estate and ensure that data is handled in line with compliance requirements. Admins can enable their organization to know its data through data classification capabilities and tools in the Microsoft Purview compliance portal, such as sensitive information types, trainable classifiers, content explorer, and activity explorer.

Identifying and classifying sensitive items that are under your organization's control is the first step in the Information Protection discipline. Microsoft Purview provides three ways of identifying items so that they can be classified:

- manually by users
- automated pattern recognition, like sensitive information types

21 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

- machine learning

Sensitive information types

Sensitive information types (SIT) are pattern-based classifiers. They have set patterns that can be used to identify them. For example, an identification number in a country/region may be based on a specific pattern, like this:

123-456-789-ABC

Microsoft Purview includes many built-in sensitive information types based on patterns that are defined by a regular expression (regex) or a function.

Examples include:

- Credit card numbers
- Passport or identification numbers
- Bank account numbers
- Health service numbers

Refer to **Sensitive information type entity definitions**[22] for a listing of available built-in sensitive information types.

Data classification in Microsoft Purview also supports the ability to create custom sensitive information types to address organization-specific requirements. For example, an organization may need to create sensitive information types to represent employee IDs or project numbers.

Also supported is exact data match (EDM) classification. EDM-based classification enables you to create custom sensitive information types that refer to exact values in a database of sensitive information.

Trainable classifiers

Trainable classifiers use artificial intelligence and machine learning to intelligently classify your data. They're most useful classifying data unique to an organization like specific kinds of contracts, invoices, or customer records. This method of classification is more about training a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching).
Two types of classifier are available:

- **Pre-trained classifiers** - Microsoft has created and pretrained many classifiers that you can start using without training them. These classifiers will appear with the status of **Ready to use**. Microsoft Purview comes with five pretrained classifiers that detect and classify things like resumes, source code, harassment, profanity, and threat (relates to committing violence or doing physical harm).
- **Custom trainable classifiers** - Microsoft supports the ability to create and train custom classifiers. They're most useful when classifying data unique to an organization, like specific kinds of contracts, invoices, or customer records.

To get a custom trainable classifier to accurately identify an item as being in a particular category of content, it must first be presented with many samples of the type of content in the category. This feeding of positive samples is known as seeding and is used to create a prediction model for the classifier.

The model gets tested to determine if the classifier can correctly distinguish between items that match the category and items that don't. The result of each prediction is manually verified, which serves as input to improve the accuracy of the prediction model.

22 https://docs.microsoft.com/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide

After the accuracy score of the model has stabilized, the classifier can be published.
Trainable classifiers can then sort through items in locations like SharePoint Online, Exchange, and OneDrive, and classify the content.

NOTE: At this time, classifiers only work with items that are not encrypted.

Understand and explore the data

Data classification can involve large numbers of documents and emails. To help administrators to easily derive insights and understanding, the overview section of the data classification pane in compliance portal provides many details at a glance, including:

- The number of items classified as sensitive information and which classifications they are.
- Details on the locations of data based on sensitivity.
- Summary of actions that users are taking on sensitive content across the organization.

Administrators can also use the content and activity explorers to gain a deeper understanding and guide their actions.

What is the content explorer?

The content explorer is available as a tab in the data classification pane of compliance portal. It enables administrators to gain visibility into the content that has been summarized in the overview pane.

Access to content explorer is highly restricted because it makes it possible to read the contents of scanned files. There are two roles that grant access to content explorer:

- Content explorer list viewer.
- Content explorer content viewer.

Anyone who wants to access content explorer must have an account in one or both of the role groups.

With content explorer, administrators get a current snapshot of individual items that have been classified across the organization. It enables administrators to further drill down into items by allowing them to access and review the scanned source content that's stored in different kinds of locations, such as Exchange, SharePoint, and OneDrive.

What is the activity explorer?

Activity explorer provides visibility into what content has been discovered and labeled, and where that content is. It makes it possible to monitor what's being done with labeled content across the organization. Admins gain visibility into document-level activities like label changes and label downgrades (such as when someone changes a label from confidential to public).

Admins use the filters to see all the details for a specific label, including file types, users, and activities. Activity explorer helps you understand what's being done with labeled content over time. Admins use activity explorer to evaluate if controls already in place are effective.

Here are a few of the activity types that can be analyzed:

- File copied to removable media
- File copied to network share
- Label applied
- Label changed

Admins can use more than 30 filters for data including:

- Location
- User
- Sensitivity label
- Retention label

The value of understanding what actions are being taken with sensitive content is that admins can see if the controls that they've already put in place, such as **data loss prevention policies**[23], are effective or not. For example, if it's discovered that a large number of items labeled *Highly Confidential* have suddenly been downgraded to *Public*, admins can update policies and act to restrict undesired behavior as a response.

Explore Data classification in the compliance portal

NOTE: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the video may not reflect the most recent updates.

Watch **data classification**[24] for information on the various data classification capabilities available in the compliance portal.

Describe sensitivity labels

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. For more information about Microsoft Purview, see the **blog announcement**[25]

Organizations must protect their data, to safeguard customers and business operations, and to meet compliance standards. Admins can enable their organization to protect its data, through capabilities and tools such as sensitivity labels and policies in the Microsoft Purview compliance portal.

Sensitivity labels

Sensitivity labels, available as part of information protection in the Microsoft Purview compliance portal, enable the labeling and protection of content, without affecting productivity and collaboration. With sensitivity labels, organizations can decide on labels to apply to content such as emails and documents, much like different stamps are applied to physical documents:

Labels are:

- **Customizable**: Admins can create different categories specific to the organization, such as Personal, Public, Confidential, and Highly Confidential.
- **Clear text**: Because each label is stored in clear text in the content's metadata, third-party apps and services can read it and then apply their own protective actions, if necessary.
- **Persistent**. After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. The label then moves with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.

Each item that supports sensitivity labels can only have one label applied to it, at any given time.

23 https://docs.microsoft.com/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide
24 https://www.microsoft.com/videoplayer/embed/RE4vx8x
25 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

Sensitivity labels can be configured to:

- **Encrypt** email only or both email and documents.
- **Mark the content** when Office apps are used. Marking the content includes adding watermarks, headers, or footers. Headers or footers can be added to emails or documents. Watermarks can be applied to documents but not to email.
- **Apply the label automatically** in Office apps or recommend a label. Admins choose the types of sensitive information to be labeled. The label can be applied automatically or configured to prompt users to apply the recommended label.
- **Protect content in containers such as sites and groups**. This label configuration doesn't result in documents being automatically labeled. Instead, the label settings protect content by controlling access to the container where documents are stored.
- **Extend sensitivity labels to third-party apps and services**. The Microsoft Purview Information Protection SDK enables third-party apps to read sensitivity labels and apply protection settings.
- **Classify content without using any protection settings**. A classification can be assigned to content (just like a sticker) that persists and roams with the content as it's used and shared. The classification can be used to generate usage reports and view activity data for sensitive content.

Label policies

After sensitivity labels are created, they need to be published to make them available to people and services in the organization. Sensitivity labels are published to users or groups through label policies. Sensitivity labels will then appear in Office apps for those users and groups. The sensitivity labels can be applied to documents and emails.
Label policies enable admins to:

- **Choose the users and groups that can see labels**. Labels can be published to specific users, distribution groups, Microsoft 365 groups in Azure Active Directory, and more.
- **Apply a default label** to all new emails and documents that the specified users and groups create. Users can always change the default label if they believe the document or email has been mislabeled.
- **Require justifications for label changes**. If a user wants to remove a label or replace it, admins can require the user to provide a valid justification to complete the action. The user will be prompted to provide an explanation for why the label should be changed.
- **Require users to apply a label (mandatory labeling)**. It ensures a label is applied before users can save their documents, send emails, or create new sites or groups.
- **Link users to custom help pages**. It helps users to understand what the different labels mean and how they should be used.

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.

Describe data loss prevention

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Office 365 Data Loss Prevention is now Microsoft Purview Data Loss Prevention. For more information about Microsoft Purview, see the **blog announcement**[26]

26 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

Data loss can harm an organization’s customers, business processes, and the organization itself. Organizations need to prevent data loss by detecting risky behavior and preventing sensitive information from being shared inappropriately. Admins can use data loss prevention policies, available in the Microsoft Purview compliance portal, to help their organization.

Microsoft Purview Data Loss Prevention (DLP) is a way to protect sensitive information and prevent its inadvertent disclosure. With DLP policies, admins can:

- **Identify, monitor, and automatically protect** sensitive information across Microsoft 365, including:
  - OneDrive for Business
  - SharePoint Online
  - Microsoft Teams
  - Exchange Online
- **Help users learn how compliance works** without interrupting their workflow. For example, if a user tries to share a document containing sensitive information, a DLP policy can send them an email notification and show them a policy tip.
- **View DLP reports** showing content that matches the organization's DLP policies. To assess how the organization is following a DLP policy, admins can see how many matches each policy has over time.

DLP policies protect content through the enforcement of rules that consist of:

- **Conditions** that the content must match before the rule is enforced.
- **Actions** that the admin wants the rule to take automatically when content that matches the conditions has been found.
- **Locations** where the policy will be applied, such as Exchange, SharePoint, OneDrive, and more.

For example, an admin can configure a DLP policy that helps detect information that's subject to a compliance regulation like the Health Insurance Portability and Accountability Act (HIPAA) across all SharePoint sites and OneDrive for Business. The admin can block the relevant documents from being shared inappropriately.

DLP policies protect information by identifying and automatically protecting sensitive data.
Here's some scenarios where DLP policies can help:

- Identify any document containing a credit card number stored in users’ OneDrive for Business accounts.
- Automatically block an email containing employee personal information from being sent outside the organization.

A policy can contain one or more rules, and each rule consists of conditions and actions at a minimum. For each rule, when the conditions are met, the actions are taken automatically. Rules can be grouped into one policy, to help simplify management and reporting. The diagram below shows how multiple rules, each with their own conditions and actions, are grouped into a single policy.



The rules inside the policy are prioritized in how they're implemented. For example, in the above diagram, rule one will be prioritized before rule two, and so on.

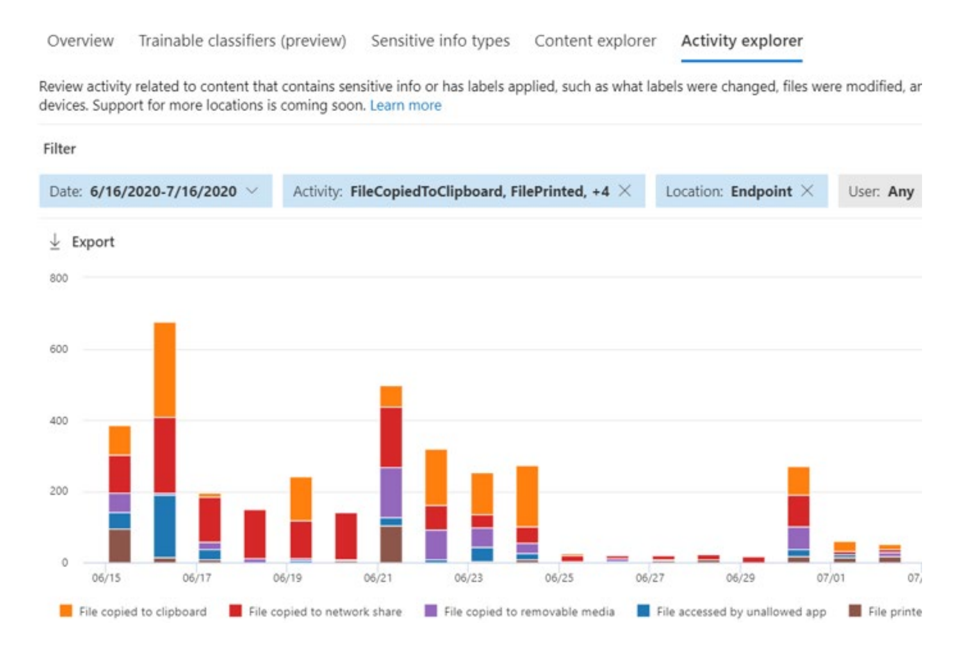
What is endpoint data loss prevention?

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices

Endpoint DLP enables admins to audit and manage activities that users complete on sensitive content. Listed below are a few examples:

- Creating an item
- Renaming an item
- Copying items to removable media
- Copying items to network shares
- Printing documents
- Accessing items using unallowed apps and browsers

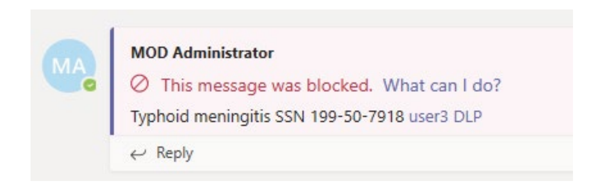
In the activity explorer, you can view information about what users are doing with sensitive content.



Admins use this information to enforce protective actions for content through controls and policies.

Data loss prevention in Microsoft Teams

Data loss prevention capabilities have been extended to Microsoft Teams chat and channel messages, including messages in private channels. With DLP, administrators can now define policies that prevent users from sharing sensitive information in a Teams chat session or channel, whether it's in a message, or a file. Just like with Exchange, Outlook, SharePoint, and OneDrive for Business, administrators can use DLP policy tips that will be displayed to the user to show them why a policy has been triggered. For example, the screenshot below shows a policy tip on a chat message that was blocked because the user attempted to share a U.S. Social Security Number.



The user can then find out more about why their message was blocked by selecting the "What can I do?" link, and take appropriate action.

Your message was blocked because it contains sensitive data

- U.S. Social Security Number (SSN)
- International Classification of Diseases (ICD-10-CM)
- International Classification of Diseases (ICD-9-CM)

This item is protected by a policy in your organization.

Here's what you can do

Override the policy and send the message, or report this to your admin if you think the message was blocked in error.

○ Override and send.

Type your justification

○ Report this to my admin. It doesn't contain sensitive data.

Cancel Confirm

With DLP policies, Microsoft Teams can help users across organizations to collaborate securely and in a way that's in line with compliance requirements.

Describe retention polices and retention labels

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. For more information about Microsoft Purview, see the **blog announcement**[27]

Retention labels and policies help organizations to manage and govern information by ensuring content is kept only for a required time, and then permanently deleted. Applying retention labels and assigning retention policies helps organizations:

- **Comply proactively with industry regulations and internal policies** that require content to be kept for a minimum time.
- **Reduce risk when there's litigation or a security breach** by permanently deleting old content that the organization is no longer required to keep.
- **Ensure users work only with content that's current and relevant to them**.
  When content has retention settings assigned to it, that content remains in its original location. People can continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy of the content is automatically kept in a secure location. The secure locations and the content are not visible to most people. In most cases, people don't even need to know that their content is subject to retention settings.

Retention settings work with the following different workloads:

- **SharePoint and OneDrive**[28]
- **Microsoft Teams**[29]
- **Yammer**[30]

27 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/
28 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide
29 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-teams?view=o365-worldwide
30 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-yammer?view=o365-worldwide

- **Exchange**[31]

When using retention policies and retention labels to assign retention settings to content, there are some points to understand about each. Listed below are just a few of the key points. For a more complete list visit **Compare capabilities for retention policies and retention labels**[32].

Retention policies

- Retention policies are used to assign the same retention settings to content at a site level or mailbox level.
- A single policy can be applied to multiple locations, or to specific locations or users.
- Items inherit the retention settings from their container specified in the retention policy. If a policy is configured to keep content, and an item is then moved outside that container, a copy of the item is kept in the workload's secured location. However, the retention settings don't travel with the content in its new location.

Retention labels

- Retention labels are used to assign retention settings at an item level, such as a folder, document, or email.
- An email or document can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content if it’s moved to a different location within your Microsoft 365 tenant.
- Admins can enable users in the organization to apply a retention label manually.
- A retention label can be applied automatically if it matches defined conditions.
- A default label can be applied for SharePoint documents.
- Retention labels support disposition review to review the content before it's permanently deleted.

Consider the following scenarios. If all documents in a SharePoint site should be kept for five years, it's more efficient to do with a retention policy than apply the same retention label to all documents in that site.

However, if some documents in that site should be kept for five years and others for 10 years, you'd need to apply a policy to the SharePoint site with a retention period of five years. You'd then apply a retention label to the individual item with a retention setting of 10 years.

Describe records management

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Records Management in Microsoft 365 is now Microsoft Purview Records Management. For more information about Microsoft Purview, see the **blog announcement**[33]

Organizations of all types require a management solution to manage regulatory, legal, and business-critical records across their corporate data. Microsoft Purview Records Management helps an organization look after their legal obligations. It also helps to demonstrate compliance with regulations, and increases efficiency with regular disposition of items that are no longer required to be kept, no longer of value, or

31 https://docs.microsoft.com/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide
32 https://docs.microsoft.com/microsoft-365/compliance/retention?view=o365-worldwide#compare-capabilities-for-retention-policies-and-retention-labels
33 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

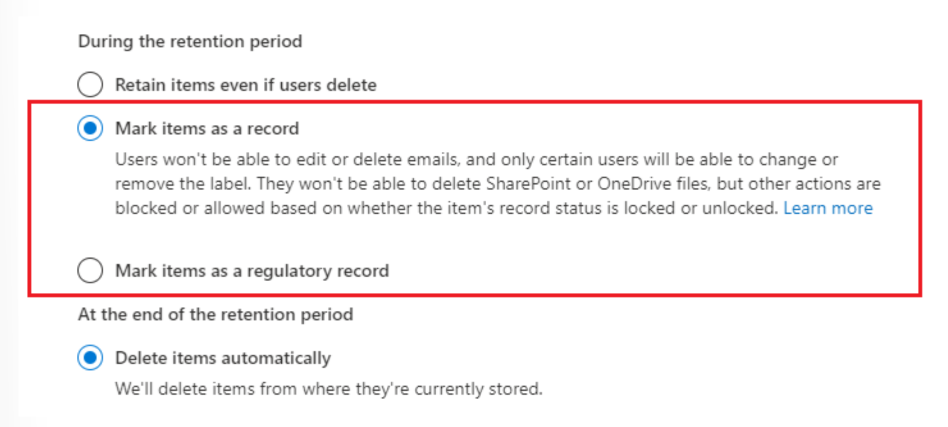
no longer required for business purposes. Microsoft Purview Records Management includes many features, including:

- Labeling content as a record.
- Establishing retention and deletion policies within the record label.
- Triggering event-based retention.
- Reviewing and validating disposition.
- Proof of records deletion.
- Exporting information about disposed items.

When content is labeled as a record, the following happens:

- Restrictions are put in place to block certain activities.
- Activities are logged.
- Proof of disposition is kept at the end of the retention period.

To enable items to be marked as records, an administrator sets up retention labels.



Items such as documents and emails can then be marked as records based on those retention labels. Items might be marked as records, but they can also be shown as regulatory records. Regulatory records provide other controls and restrictions such as:

- A regulatory label can't be removed when an item has been marked as a regulatory record.
- The retention periods can't be made shorter after the label has been applied.

For more information on comparing, use the **Compare restrictions for what actions are allowed or blocked section**[34] of the documentation.

The most important difference is that if content has been marked as a regulatory record, nobody, not even a global administrator, can remove the label. Marking an item as a regulatory record can have irreversible consequences, and should only be used when necessary. As a result, this option isn't available by default, and has to be enabled by the administrator using PowerShell.

34 https://docs.microsoft.com/microsoft-365/compliance/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked

Common use cases for records management

The capabilities of Microsoft Purview Records Management are flexible. There are different ways in which records management can be used across an organization, including:

- Enabling administrators and users to manually apply retention and deletion actions for documents and emails.
- Automatically applying retention and deletion actions to documents and emails.
- Enabling site admins to set default retain and delete actions for all content in a SharePoint library, folder, or document set.
- Enabling users to automatically apply retain and delete actions to emails by using Outlook rules.

To ensure records management is used correctly across the organization, administrators can work with content creators to put together training materials. Documentation should explain how to apply labels to drive usage, and ensure a consistent understanding.

Knowledge check

Multiple choice

Item 1. Which part of the concept of know your data, protect your data, prevent data loss, and govern your data addresses the need for organizations to automatically retain, delete, store data and records in a compliant manner?

- ☐ Know your data.
- ☐ Prevent data loss.
- ☐ Govern your data.

Multiple choice

Item 2. As part of a new data loss prevention policy, the compliance admin needs to be able to identify important information such as credit card numbers, across the organization's data. How can the admin address this requirement?

- ☐ Use activity explorer.
- ☐ Use sensitivity labels.
- ☐ Use sensitive information types.

Multiple choice

Item 3. Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

- ☐ Use the content explorer.
- ☐ Use sensitivity labels.
- ☐ Use records management.

Multiple choice

Item 4. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement?

- ☐ Use data loss prevention policies.
- ☐ Use records management capabilities.
- ☐ Use retention policies.

Multiple choice

Item 5. Due to a certain regulation, your organization must now keep hold of all documents in a specific SharePoint site that contains customer information for five years. How can this requirement be implemented?

- ☐ Use sensitivity labels.
- ☐ Use the content explorer.
- ☐ Use retention policies.

Summary and resources

You've explored how Microsoft Purview capabilities like data classification, records management, and data loss prevention can help provide information protection and data lifecycle management across an organization.

Without these capabilities, an organization's information could be at risk, and it might not be compliant with legal and regulatory standards. Microsoft 365 information protection and governance capabilities can help organizations address their compliance needs and mitigate risk.

Now that you've completed this lesson, you'll be able to:

- Describe data classification capabilities.
- Describe data loss prevention.
- Describe records management.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Know your data - data classification overview**[35]
- **Get started with content explorer**[36]
- **Learn about sensitivity labels**[37]
- **Get started with activity explorer**[38]
- **Learn about retention policies and retention labels**[39]

35 https://docs.microsoft.com/microsoft-365/compliance/data-classification-overview?view=o365-worldwide
36 https://docs.microsoft.com/microsoft-365/compliance/data-classification-content-explorer?view=o365-worldwide
37 https://docs.microsoft.com/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
38 https://docs.microsoft.com/microsoft-365/compliance/data-classification-activity-explorer?view=o365-worldwide
39 https://docs.microsoft.com/microsoft-365/compliance/retention?view=o365-worldwide

- **Govern your data with Microsoft Purview**[40]
- **Learn about records management**[41]

40 https://docs.microsoft.com/microsoft-365/compliance/manage-information-governance?view=o365-worldwide
41 https://docs.microsoft.com/microsoft-365/compliance/records-management?view=o365-worldwide

Describe the insider risk capabilities in Microsoft Purview

Introduction

Organizations understand that risks can come from insiders, like contractors, or even employees. There's always a risk that people might share information with competitors after leaving the company. Organizations need to ensure that they're protected from these kinds of risks.

In this lesson, you'll learn how insider risk management, communication compliance, and information barriers in Microsoft Purview can help you protect your organization.

After completing this lesson, you'll be able to:

- Describe insider risk management.
- Describe communication compliance.
- Describe information barriers.

Describe insider risk management

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft 365 Insider Risk Management is now Microsoft Purview Insider Risk Management. For more information about Microsoft Purview, see the **blog announcement**[42]

Microsoft Purview Insider Risk Management is a solution that helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities. Insider risk management is available in the Microsoft Purview compliance portal.

Managing and minimizing risk in an organization starts with understanding the types of risks found in the modern workplace. Some risks are driven by external events and factors, and are outside an organization's direct control. Other risks are driven by internal events and employee activities that can be eliminated and avoided. Some examples are risks from illegal, inappropriate, unauthorized, or unethical behavior and actions by employees and managers. These behaviors can lead to a broad range of internal risks from employees:

- Leaks of sensitive data and data spillage
- Confidentiality violations
- Intellectual property (IP) theft
- Fraud
- Insider trading
- Regulatory compliance violations

Insider risk management is centered around the following principles:

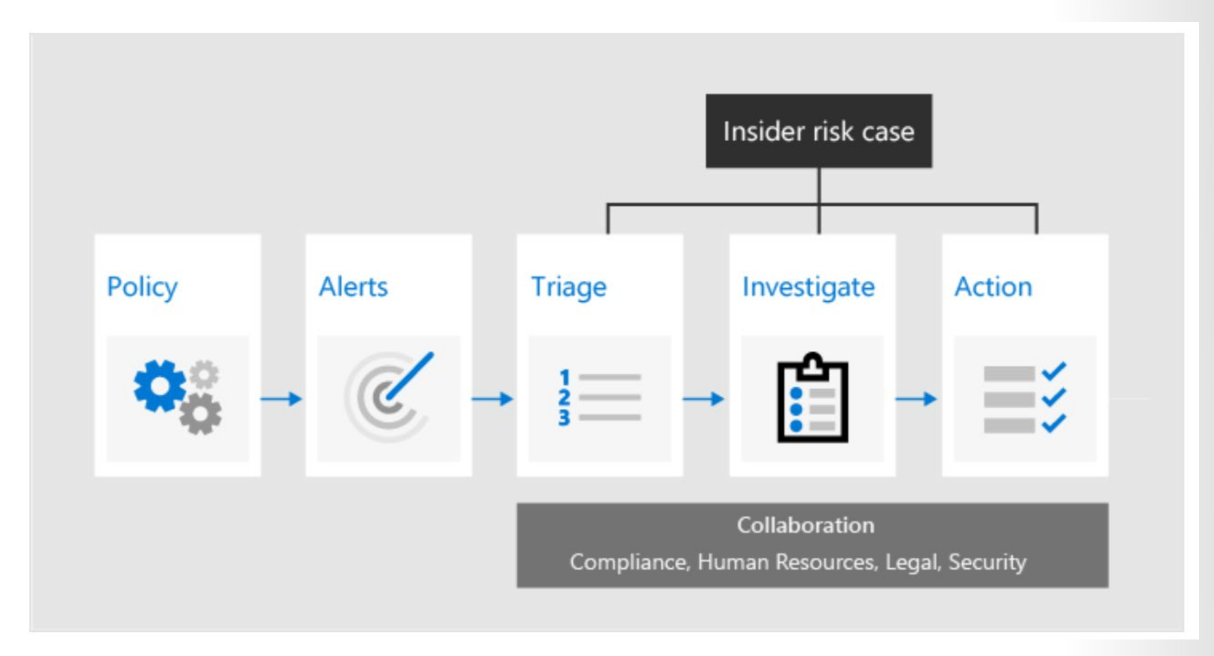
- **Transparency**: Balance user privacy versus organization risk with privacy-by-design architecture.
- **Configurable**: Configurable policies based on industry, geographical, and business groups.
- **Integrated**: Integrated workflow across Microsoft Purview compliance solutions.

42 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

- **Actionable**: Provides insights to enable user notifications, data investigations, and user investigations.

Insider risk management workflow

Insider risk management helps organizations to identify, investigate, and address internal risks. With focused policy templates, comprehensive activity signaling across Microsoft 365, and a flexible workflow, organizations can take advantage of actionable insights to help identify and resolve risky behavior quickly.
Identifying and resolving internal risk activities and compliance issues with insider risk management in Microsoft Purview is achieved using the following workflow:



- **Policies** - Insider risk management policies are created using predefined templates and policy conditions that define what risk indicators are examined in Microsoft 365 feature areas. These conditions include how indicators are used for alerts, what users are included in the policy, which services are prioritized, and the monitoring time period.
- **Alerts** - Alerts are automatically generated by risk indicators that match policy conditions and are displayed in the **Alerts dashboard**. This dashboard enables a quick view of all alerts needing review, open alerts over time, and alert statistics for the organization.
- **Triage** - New activities that need investigation automatically generate alerts that are assigned a *Needs review* status. Reviewers in the organization can quickly identify these alerts and scroll through each to evaluate and triage. Alerts are resolved by opening a new case, assigning the alert to an existing case, or dismissing the alert. As part of the triage process, reviewers can view alert details for the policy match, view user activity associated with the match, see the severity of the alert, and review user profile information.
- **Investigate** - Cases are created for alerts that require deeper review and investigation of the details and circumstances around the policy match. The **Case dashboard** provides an all-up view of all active cases, open cases over time, and case statistics for the organization. Selecting a case on the dashboard opens it for investigation and review. This area is where risk activities, policy conditions, alerts details, and user details are synthesized into an integrated view for reviewers.

- **Action** - After cases are investigated, reviewers can quickly act to resolve the case or collaborate with other risk stakeholders in the organization.
  - Actions can be as simple as sending a notification when employees accidentally or inadvertently violate policy conditions.
  - In more serious cases, reviewers may need to share the insider risk management case information with other reviewers in the organization. Escalating a case for investigation makes it possible to transfer data and management of the case to eDiscovery (Premium) in Microsoft Purview.

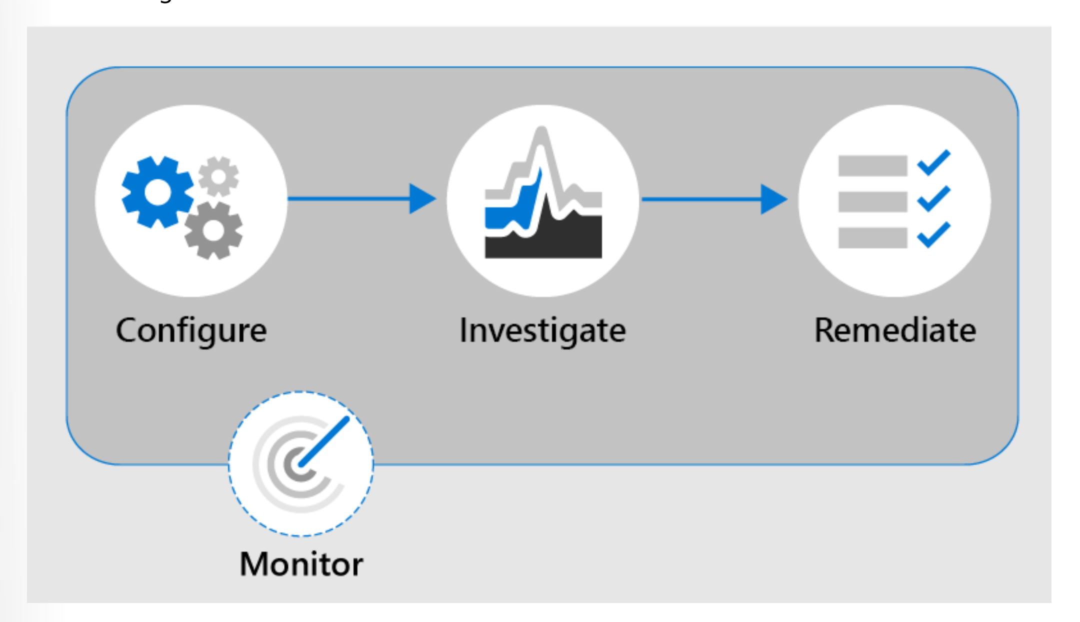
Insider risk management can help you detect, investigate, and take action to mitigate internal risks in your organization in several common scenarios. These scenarios include data theft by employees, the intentional, or unintentional leak of confidential information, offensive behavior, and more.

Describe communication compliance

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft 365 Communication Compliance is now Microsoft Purview Communication Compliance. For more information about Microsoft Purview, see the **blog announcement**[43]

Microsoft Purview Communication Compliance in Microsoft Purview compliance portal helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages. Predefined and custom policies in communication compliance make it possible to scan internal and external communications for policy matches so they can be examined by chosen reviewers.

Identifying and resolving compliance issues with communication compliance in Microsoft Purview uses the following workflow:



- **Configure** – in this step, admins identify compliance requirements and configure applicable communication compliance policies.

43 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

- **Investigate** – admins look deeper into the issues detected when matching your communication compliance policies. Tools and steps that help include alerts, issue management to help remediation, document reviews, reviewing user history, and filters.
- **Remediate** – remediate communications compliance issues. Options include resolving an alert, tagging a message, notifying the user, escalating to another reviewer, marking an alert as a false positive, removing a message in Teams, and escalating for investigation.
- **Monitor** – Keeping track and managing compliance issues identified by communication compliance policies spans the entire workflow process. Communication compliance dashboard widgets, export logs, and events recorded in the unified audit logs can be used to continually evaluate and improve your compliance posture.

Communication compliance enables reviewers to investigate scanned emails, and messages across Microsoft Teams, Exchange Online, Yammer, or third-party communications in an organization, taking appropriate remediation actions to make sure they're compliant with the organization's message standards.

Some important compliance areas where communication compliance policies can assist with reviewing messages include:

- **Corporate policies** - Users have to follow corporate policies like usage and ethical standards in their day-to-day business communications. With communication compliance, admins can scan user communications across the organization for potential concerns of offensive language or harassment.
- **Risk management** - Communication compliance can help admins scan for unauthorized communication about projects that are considered to be confidential, such as acquisitions, earnings disclosures, and more.
- **Regulatory compliance** - Most organizations are expected to follow some regulatory compliance standards during their day-to-day operations. For example, a regulation might require organizations in the finance sector to review communications of its brokers to safeguard against potential insider trading, money laundering, or bribery. Communication compliance enables the organization to scan and report on these types of communications in a way that meets their requirements.

For a walk-through of the communication compliance capability, select the link below. **NOTE**: The user interface (UI) in Microsoft 365 is continually evolving so the UI shown in the video may not reflect the most recent updates.

Communication Compliance: Solution tutorial to identify inappropriate communication and quickly take action[44].

Communication compliance is a powerful tool, that can help maintain and safeguard your staff, your data and your organization.

Describe information barriers

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft 365 Information Barriers is now Microsoft Purview Information Barriers. For more information about Microsoft Purview, see the **blog announcement**[45]

Microsoft 365 provides organizations with powerful communication and collaboration capabilities. However, an organization might want to restrict communications between some groups to avoid a conflict of interest from occurring in the organization, or to restrict communications between certain

44 https://www.microsoft.com/videoplayer/embed/RE4xlaF
45 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

people to safeguard internal information. With information barriers, the organization can restrict communications among specific groups of users.

It's important to note that information barriers *only support two-way restrictions*. One-way restrictions, such as marketing, can communicate with day traders but day traders who can't communicate with marketing are *not supported*.

Information barriers are policies that admins can configure to prevent individuals or groups from communicating with each other. When information barrier policies are in place, people who shouldn't communicate with other specific users can't find, select, chat, or call those users. With information barriers, checks are in place to prevent unauthorized communication.

Here are some examples of how information barriers can be applied:

- **Education**: Students in one school can't look up contact details for students of other schools.
- **Legal**: Maintaining confidentiality of data obtained by the lawyer of one client from being accessed by a lawyer for the same firm representing a different client.
- **Professional services**: A group of people in a company is only able to chat with a client or specific customer via federation or guest access during a customer engagement.

Information barriers are supported in solutions like Microsoft Teams, OneDrive for Business, SharePoint Online, and more.

Information barriers in Microsoft Teams

In Microsoft Teams, information barrier policies determine and prevent the following kinds of unauthorized communications:

- Searching for a user
- Adding a member to a team
- Starting a chat session with someone
- Starting a group chat
- Inviting someone to join a meeting
- Sharing a screen
- Placing a call
- Sharing a file with another user
- Access to file through sharing link

If the people involved are included in an information barrier policy to prevent the activity, they cannot continue. Potentially, everyone included in an information barrier policy can be blocked from communicating with others in Microsoft Teams. When people affected by information barrier policies are part of the same team or group chat, they might be removed from those chat sessions and further communication with the group might not be allowed.

To learn more about the user experience with information barriers, visit **information barriers in Microsoft Teams**[46].

46 https://docs.microsoft.com/MicrosoftTeams/information-barriers-in-teams

Knowledge check

Multiple choice

Item 1. The compliance admin for the organization wants explain the importance of Microsoft Purview Insider Risk Management, to the business leaders? What use case would apply?

- ☐ To identify and protect against risks like an employee sharing confidential information.
- ☐ To identify and protect against malicious software across your network, such as ransomware.
- ☐ To identify and protect against devices shutting down at critical moments.

Multiple choice

Item 2. To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need?

- ☐ Use Policy Compliance in Microsoft 365.
- ☐ Use Microsoft Purview Communication Compliance.
- ☐ Use Microsoft Purview Information Barriers.

Multiple choice

Item 3. An organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need?

- ☐ Use Microsoft Purview Communication Compliance.
- ☐ Use activity explorer.
- ☐ Use Microsoft Purview Information Barriers.

Summary and resources

There are various capabilities available from Microsoft Purview to help protect organizations from data leaks or inappropriate communication, from company insiders.

Now that you've completed this lesson, you'll be able to:

- Describe insider risk management.
- Describe communication compliance.
- Describe information barriers.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Learn about insider risk management**[47]
- **Get started with communication compliance**[48]

47 https://docs.microsoft.com/microsoft-365/compliance/insider-risk-management?view=o365-worldwide
48 https://docs.microsoft.com/microsoft-365/compliance/communication-compliance-configure?view=o365-worldwide#before-you-begin

- **Information barriers**[49]

49 https://docs.microsoft.com/microsoft-365/compliance/information-barriers-solution-overview?view=o365-worldwide

Describe the eDiscovery and audit capabilities of Microsoft Purview

Introduction

Organizations may need to identify, collect, and/or audit information for legal, regulatory, or business reasons. With today's volume and variety of data, it's vital that an organization can do this in an efficient and timely manner. The eDiscovery and audit capabilities in Microsoft Purview can help organizations to achieve this goal.

Learn how the eDiscovery and audit capabilities of Microsoft Purview help organizations find relevant data quickly.

After completing this lesson, you'll be able to:

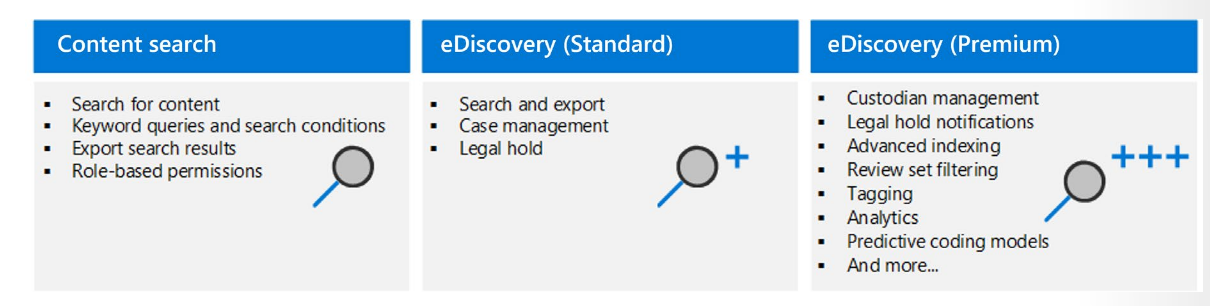
- Describe the eDiscovery solutions in Microsoft Purview.
- Describe the auditing solutions in Microsoft Purview.

Describe the eDiscovery solutions in Microsoft Purview

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Office 365 core eDiscovery is now Microsoft Purview eDiscovery (Standard). Office 365 Advanced eDiscovery is now Microsoft Purview eDiscovery (Premium). For more information about Microsoft Purview, see the **blog announcement**[50]

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use eDiscovery tools in Microsoft Purview to search for content in Exchange Online, OneDrive for Business, SharePoint Online, Microsoft Teams, Microsoft 365 Groups, and Yammer teams. You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use eDiscovery cases to identify, hold, and export content found in mailboxes and sites.

Microsoft Purview provides three eDiscovery solutions: Content search, eDiscovery (Standard), and eDiscovery (Premium).



- **Content Search**. Use the Content search tool to search for content across Microsoft 365 data sources and then export the search results to a local computer.
- **eDiscovery (Standard)**. The eDiscovery (Standard) solution builds on the basic search and export functionality of Content search by enabling you to create eDiscovery cases and assign eDiscovery

50 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

managers to specific cases. The eDiscovery (Standard) solution also lets you associate searches and exports with a case and lets you place an eDiscovery hold on content locations relevant to the case.

- **eDiscovery (Premium)**. The eDiscovery (Premium) solution builds on the existing capabilities in eDiscovery (Standard). In addition, eDiscovery (Premium) provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It lets legal teams manage custodians, people that you've identified as people of interest in the case, and the workflow to communicate with custodians. It allows you to collect and copy data into review sets, where you can filter, search, and tag content so you can identify and focus on content that's most relevant. The eDiscovery (Premium) solution provides analytics and machine learning-based predictive coding models to further narrow to scope of your investigation to the most relevant content.

Subscriptions that support eDiscovery (Standard) also support Content search. Subscriptions that support eDiscovery (Premium) also support Content search and eDiscovery (Standard).

To access any of the eDiscovery-related tools, a user must be assigned the appropriate permissions. Specifically, a user must be added as a member of the eDiscovery Manager role group in the Microsoft Purview compliance portal.

Describe the audit solutions in Microsoft Purview

NOTE: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Microsoft 365 Audit is now Microsoft Purview Audit (Standard). Microsoft 365 Advanced Audit is now Microsoft Purview Audit (Premium). For more information about Microsoft Purview, see the **blog announcement**[51]

Auditing solutions in Microsoft Purview help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Microsoft Purview provides two auditing solutions: Audit (Standard) and Audit (Premium).

- **Audit (Standard)**. Audit (Standard) provides with you with the ability to log and search for audited activities and power your forensic, IT, compliance, and legal investigations. Audit (Standard) is turned on by default for all organizations with the appropriate subscription. You can search for a wide-range of audited activities that occur in most of the Microsoft 365 services in your organization. Audit

51 https://www.microsoft.com/security/blog/2022/04/19/the-future-of-compliance-and-data-governance-is-here-introducing-microsoft-purview/

records can also be retrieved using the Office 365 Management Activity API. You can export the audit records returned by the search, to a CSV file, enabling further analysis using Microsoft Excel or Excel Power Query. In Audit (Standard), records are retained for 90 days.

- **Audit (Premium)**. Audit (Premium) builds on the capabilities of Audit (Standard). Audit (Premium) provides audit log retention policies and longer retention of audit records. It provides audit records for high-value crucial events that can help your organization investigate possible security or compliance breaches and determine the scope of compromise. Audit (Premium) also provides organizations with more bandwidth to access auditing logs through the Office 365 Management Activity API.

It can take anywhere from 30 minutes to 24 hours after an event occurs for the corresponding audit log record to be returned in the results of an audit log search.

Licensing for Audit (Standard) or Audit (Premium) requires the appropriate organization-level subscription and corresponding per-user licensing. For additional information on licensing requirements, visit the Learn more section in the Summary and resources unit.

Admins and members of investigation teams must be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center.

Knowledge check

Multiple choice

Item 1. A new admin has joined the compliance team and needs access to eDiscovery (Standard) to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned?

☐ Add them as a member of the eDiscovery Manager role group.

☐ Add them as a member of the eDiscovery review role.

☐ Add them as a member of the eDiscovery custodian role.

Multiple choice

Item 2. The compliance admin needs to be able to collect and copy data into review sets and to be able filter, search, and tag content, which solution can best address his need?

☐ Audit (Standard)

☐ Search

☐ eDiscovery (Premium)

Multiple choice

Item 3. The compliance team needs to preserve the records for high-value crucial events that can help the organization investigate possible security or compliance breaches and determine the scope of compromise. Which solution can best address that need?

- ☐ Audit (Premium).
- ☐ Search.
- ☐ eDiscovery (Standard).

Summary and resources

The eDiscovery and audit solutions in Microsoft Purview can help organizations identify, collect, and audit information in a rapid and effective manner, to meet legal requirements.

Now that you've completed this lesson, you'll be able to:

- Describe the eDiscovery solutions in Microsoft Purview.
- Describe the auditing solutions in Microsoft Purview.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **Microsoft Purview eDiscovery solutions**[52]
- **Search for content using the Content search tool**[53]
- **Get started with eDiscovery (Standard) in Microsoft Purview**[54]
- **Overview of Microsoft Purview eDiscovery (Premium)**[55]
- **Auditing solutions in Microsoft Purview**[56]
- **Microsoft Purview Audit (Premium)**[57]
- **Turn audit log search on or off**[58]

52 https://docs.microsoft.com/microsoft-365/compliance/ediscovery?view=o365-worldwide
53 https://docs.microsoft.com/microsoft-365/compliance/search-for-content?view=o365-worldwide
54 https://docs.microsoft.com/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide
55 https://docs.microsoft.com/microsoft-365/compliance/overview-ediscovery-20?view=o365-worldwide
56 https://docs.microsoft.com/microsoft-365/compliance/auditing-solutions-overview?view=o365-worldwide
57 https://docs.microsoft.com/microsoft-365/compliance/advanced-audit?view=o365-worldwide
58 https://docs.microsoft.com/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide

Describe the resource governance capabilities in Azure

Introduction

Azure has the capabilities that admins need to ensure that resources are governed properly, that they're secure, and in line with the organization's compliance requirements.

In this lesson, you'll learn about the resource governance capabilities available for Azure.

After completing this lesson, you'll be able to:

- Describe Azure Policy.
- Describe Azure Blueprints.
- Describe Microsoft Purview.

Describe Azure policy

Azure Policy is designed to help enforce standards and assess compliance across your organization. Through its compliance dashboard, you can access an aggregated view to help evaluate the overall state of the environment. You can drill down to a per-resource, or per-policy level granularity. You can also use capabilities like bulk remediation for existing resources and automatic remediation for new resources, to resolve issues rapidly and effectively. Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.

Azure Policy evaluates all resources in Azure and Arc enabled resources (specific resource types hosted outside of Azure).

Azure Policy evaluates whether the properties of resources match with business rules. These business rules are described using **JSON**[59] format, and referred to as **policy definitions**[60]. For simplified management, you can group together multiple business rules to form a single **policy initiative**[61]. After business rules have been formed, you can assign the policy definition, or policy initiative, to any scope of resources that are supported, such as management groups, subscriptions, resource groups, or individual resources.

Evaluation outcomes

Azure Policy evaluates resources at specific times during the resource lifecycle and the policy assignment lifecycle, and for regular ongoing compliance evaluation. The following events or times will trigger an evaluation:

- A resource has been created, deleted, or updated in scope with a policy assignment.
- A policy or an initiative is newly assigned to a scope.
- A policy or an initiative that's been assigned to a scope is updated.
- The standard compliance evaluation cycle (happens once every 24 hours).

Organizations will vary in how they respond to non-compliant resources. Here are some examples:

- Deny a change to a resource.

59 https://docs.microsoft.com/azure/governance/policy/concepts/definition-structure
60 https://docs.microsoft.com/azure/governance/policy/overview#policy-definition
61 https://docs.microsoft.com/azure/governance/policy/overview#initiative-definition

- Log changes to a resource.
- Alter a resource before or after a change.
- Deploy related compliant resources.

With Azure Policy, responses like these are made possible by using **effects**[62], which are specified in policy definitions.

What's the difference between Azure Policy and Azure role-based access control (RBAC)?

It's important not to confuse Azure Policy and Azure RBAC. You use Azure Policy to ensure that the resource state is compliant to your organization's business rules, no matter who made the change or who has permission to make changes. Azure Policy will evaluate the state of a resource, and act to ensure the resource stays compliant.

Azure RBAC focuses instead on managing user actions at different scopes. Azure RBAC manages who has access to Azure resources, what they can do with those resources, and what areas they can access. If actions need to be controlled, then you would use Azure RBAC. If an individual has access to complete an action, but the result is a non-compliant resource, Azure Policy still blocks the action.

Azure RBAC and Azure Policy should be used together to achieve full scope control in Azure.

Describe what is Azure Blueprints

Azure Blueprints provide a way to define a repeatable set of Azure resources. Azure Blueprints enable development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance requirements. Teams can also provision Azure resources across several subscriptions simultaneously, meaning they can achieve shorter development times and quicker delivery.

Azure Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

Blueprint objects are replicated to multiple Azure regions. This replication provides low latency, high availability, and consistent access to your blueprint objects, whatever region Azure Blueprints deploys your resources to.

With Azure Blueprints, the relationship between the blueprint definition (*what should be deployed*) and the blueprint assignment (*what was deployed*) is preserved. This connection supports improved tracking and auditing of deployments.

Azure Blueprints helps ensure Azure resources are deployed in a way that's in line with compliance requirements. However, a service like Azure Policy should be used to continuously monitor resources and ensure a continuation with compliance requirements.

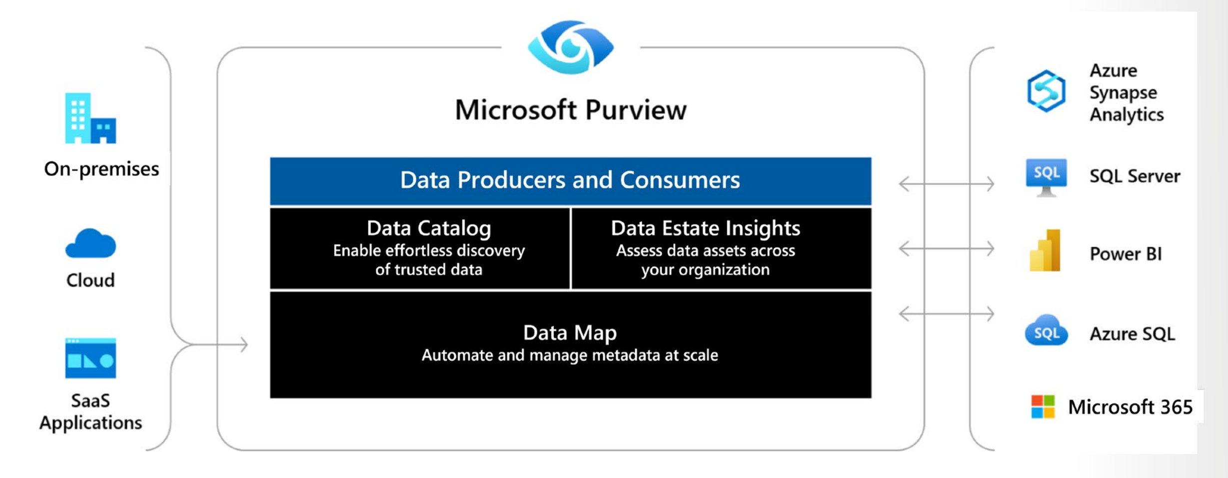
62 https://docs.microsoft.com/azure/governance/policy/concepts/effects

Describe Microsoft Purview

An organization's data is constantly growing and users are storing and sharing data in new directions. For security and compliance administrators, the task of discovering, protecting, and governing sensitive data is one that never ends. The growth of data, also represents challenges for data consumers who might be unaware of a data source. For data producers, those who are responsible for producing and maintaining information assets, creating and maintaining documentation for data sources is complex and time-consuming. Restricting access to data sources and ensuring that data consumers know how to request access is an ongoing challenge.

Microsoft Purview is designed to address the challenges associated with the rapid growth of data and to help enterprises get the most value from their information assets. Microsoft Purview is a unified data governance service that helps organizations manage and govern their on-premises, multi-cloud, and software-as-a-service (SaaS) data. With Microsoft Purview, organization can create a holistic, up-to-date map of the organization's data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Security administrators and data curators can secure and manage their data estate. Data consumers are empowered to find valuable, trustworthy data.

Microsoft Purview automates data discovery by providing data scanning and classification as a service for assets across the organization's data estate. Metadata and descriptions of discovered data assets are integrated into a holistic map of the data estate. Atop this map, there are purpose-built apps that create environments for data discovery, access management, and insights about the organization's data landscape.



Data Map

Microsoft Purview Data Map provides the foundation for data discovery and data governance. By scanning registered data sources, Azure Purview Data Map is able to capture metadata about enterprise data, to identify and classify sensitive data. Microsoft Purview supports Azure data sources and various data source categories including databases, file storage, and applications and services from third parties.

Data Catalog

With the Microsoft Purview Data Catalog, business and technical users can quickly and easily find relevant data using a search experience with filters based on various lenses like glossary terms, classifications, sensitivity labels and more.

Data Estate Insights

With the Microsoft Purview Data Estate Insights, data officers and security officers can get a bird's eye view and at a glance understand what data is actively scanned, where sensitive data is, and how it moves.

Knowledge check

Multiple choice

Item 1. Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization's compliance requirements?

- ☐ Azure Policy
- ☐ Azure Rapid Build
- ☐ Azure Blueprints

Multiple choice

Item 2. As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use?

- ☐ Use Azure role-based access control (RBAC).
- ☐ Use Azure Policy.
- ☐ Use Azure resource locks.

Multiple choice

Item 3. Which application of Microsoft Purview is used to capture metadata about enterprise data, to identify and classify sensitive data?

- ☐ Data Catalog.
- ☐ Data Map.
- ☐ Data Estate Insights.

Summary and resources

You've seen how admins can use the resource governance capabilities in Azure to ensure that resources for their organization are governed properly, so that they're secure, and in line with the organization's compliance requirements.

Now that you've completed this lesson, you'll be able to:

- Describe Azure Policy.
- Describe Azure Blueprints.
- Describe Microsoft Purview.

Learn more

To learn more about any of the topics covered in this lesson, visit these links:

- **What is Azure Policy?**[63]
- **What is Azure Blueprints?**[64]
- **What is Microsoft Purview?**[65]

63 https://docs.microsoft.com/azure/governance/policy/overview
64 https://docs.microsoft.com/azure/governance/blueprints/overview
65 https://docs.microsoft.com/azure/purview/overview

Answers

Multiple choice

Item 1. When browsing Microsoft compliance documentation in the Service Trust Portal, you have found several documents that are specific to your industry. What is the best way of ensuring you keep up to date with the latest updates?

■ Save the documents to your My Library.

☐ Print each document so you can easily refer to them.

☐ Download each document.

Explanation
By saving the documents to your My Library you will be prompted to say when you want to be notified of updates.

Multiple choice

Item 2. Microsoft's approach to privacy is built on six principles: Three of the principles are strong legal protections for privacy, no content-based targeting, and benefits to customers from any data we collect. Identify the three other principles that are part of Microsoft's approach to privacy.

■ Customer control, transparency, and security.

☐ Shared responsibility, transparency, and security.

☐ Customer control, transparency, and zero trust.

Explanation
The foundation of Microsoft's approach to privacy is built on the following six principles: customer control, transparency, security, strong legal protections for privacy, no content-based targeting, and benefits to customers from any data we collect.

Multiple choice

Item 3. Which solution in Microsoft Priva provides visibility into your organization's data and policy templates for reducing risks?

■ Privacy Risk Management.

☐ Subject Rights Request.

☐ Compliance score.

Explanation
Priva's capabilities are available through two solutions: **Priva Privacy Risk Management***, which provides visibility into your organization's data and policy templates for reducing risks; and* **Priva Subject Rights Requests***, which provides automation and workflow tools for fulfilling data requests.*

Multiple choice

Item 1. A new admin has joined the team and needs to be able to access the Microsoft Purview compliance portal. Which of the following roles could the admin use to access the compliance portal?

■ Compliance Administrator role

☐ Helpdesk Administrator role

☐ User Administrator role

Explanation
The Compliance Administrator role is one of the multiple roles you can use to access the compliance portal.

Multiple choice

Item 2. Your new colleagues on the admin team are unfamiliar with the concept of shared controls in Compliance Manager. How would the concept of shared controls be explained?

- ☐ Controls that both external regulators and Microsoft share responsibility for implementing.
- ☐ Controls that both your organization and external regulators share responsibility for implementing.
- ■ Controls that both your organization and Microsoft share responsibility for implementing.

Explanation
Both your organization and Microsoft work together to implement shared controls.

Multiple choice

Item 3. A customer has requested a presentation on how the Microsoft Purview compliance portal can help improve their organization’s compliance posture. The presentation will need to cover Compliance Manager and compliance score. What is the difference between Compliance Manager and compliance score?

- ■ Compliance Manager is an end-to-end solution in the Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.
- ☐ Compliance Manager is an end-to-end solution in Microsoft Purview compliance portal to enable admins to manage and track compliance activities. Compliance score is a score the organization receives from regulators for successful compliance.
- ☐ Compliance Manager is the regulator who will manage your compliance activities. Compliance score is a calculation of the overall compliance posture across the organization.

Explanation
Compliance Manager provides admins with the capabilities to understand and improve their compliance score so that they can ultimately improve the organization’s compliance posture and help it to stay in line with its compliance requirements..

Multiple choice

Item 1. Which part of the concept of know your data, protect your data, prevent data loss, and govern your data addresses the need for organizations to automatically retain, delete, store data and records in a compliant manner?

- ☐ Know your data.
- ☐ Prevent data loss.
- ■ Govern your data.

Explanation
Capabilities like retention policies, retention labels, and records management enable organizations to govern their data.

Multiple choice

Item 2. As part of a new data loss prevention policy, the compliance admin needs to be able to identify important information such as credit card numbers, across the organization's data. How can the admin address this requirement?

- ☐ Use activity explorer.
- ☐ Use sensitivity labels.
- ■ Use sensitive information types.

Explanation
Microsoft provides built-in sensitive information types that you can use to identify data such as credit card numbers.

Multiple choice

Item 3. Within the organization, some emails are confidential and should be encrypted so that only authorized users can read them. How can this requirement be implemented?

- ☐ Use the content explorer.
- ■ Use sensitivity labels.
- ☐ Use records management.

Explanation
Sensitivity labels help ensure that emails can only be decrypted only by users authorized by the label's encryption settings.

Multiple choice

Item 4. Your organization uses Microsoft Teams to collaborate on all projects. The compliance admin wants to prevent users from accidentally sharing sensitive information in a Microsoft Teams chat session. What capability can address this requirement?

- ■ Use data loss prevention policies.
- ☐ Use records management capabilities.
- ☐ Use retention policies.

Explanation
With data loss prevention policies, administrators can now define policies that can prevent users from sharing sensitive information in a Microsoft Teams chat session or Teams channel, whether this information is in a message, or in a file.

Multiple choice

Item 5. Due to a certain regulation, your organization must now keep hold of all documents in a specific SharePoint site that contains customer information for five years. How can this requirement be implemented?

- ☐ Use sensitivity labels.
- ☐ Use the content explorer.
- ■ Use retention policies.

Explanation
You can use retention policies to define data retention for all documents in a SharePoint site.

Multiple choice

Item 1. The compliance admin for the organization wants explain the importance of Microsoft Purview Insider Risk Management, to the business leaders? What use case would apply?

■ To identify and protect against risks like an employee sharing confidential information.

☐ To identify and protect against malicious software across your network, such as ransomware.

☐ To identify and protect against devices shutting down at critical moments.

Explanation
Use Microsoft Purview Insider Risk Management to identify and protect against risks like an employee sharing confidential information.

Multiple choice

Item 2. To comply with corporate policies, the compliance admin needs to be able to identify and scan for offensive language across the organization. What solution can the admin implement to address this need?

☐ Use Policy Compliance in Microsoft 365.

■ Use Microsoft Purview Communication Compliance.

☐ Use Microsoft Purview Information Barriers.

Explanation
Microsoft Purview Communication Compliance helps minimize communication risks by enabling you to detect, capture, and take remediation actions for inappropriate messages in the organization.

Multiple choice

Item 3. An organization has many departments that collaborate through Microsoft Teams. To comply with business policies, the IT organization needs to make sure that users from one particular department are limited in their access and interactions with other departments. What solution can address this need?

☐ Use Microsoft Purview Communication Compliance.

☐ Use activity explorer.

■ Use Microsoft Purview Information Barriers.

Explanation
With Microsoft Purview Information Barriers, you're able to restrict communications among specific groups of users when necessary.

Multiple choice

Item 1. A new admin has joined the compliance team and needs access to eDiscovery (Standard) to be able to add and remove members, create and edit searches, and export content from a case. To which role should the admin be assigned?

■ Add them as a member of the eDiscovery Manager role group.

☐ Add them as a member of the eDiscovery review role.

☐ Add them as a member of the eDiscovery custodian role.

Explanation
Members of this role group can create and manage eDiscovery cases. They can also add and remove members, place an eDiscovery hold on users, create and edit searches, and export content from an eDiscovery case.

Multiple choice

Item 2. The compliance admin needs to be able to collect and copy data into review sets and to be able filter, search, and tag content, which solution can best address his need?

☐ Audit (Standard)

☐ Search

■ eDiscovery (Premium)

Explanation
eDiscovery (Premium) allows you to collect and copy data into review sets, where you can filter, search, and tag content so you can identify and focus on content that's most relevant.

Multiple choice

Item 3. The compliance team needs to preserve the records for high-value crucial events that can help the organization investigate possible security or compliance breaches and determine the scope of compromise. Which solution can best address that need?

■ Audit (Premium).

☐ Search.

☐ eDiscovery (Standard).

Explanation
Audit (Premium) helps organizations to conduct forensic and compliance investigations by providing access to these crucial events.

Multiple choice

Item 1. Which tool can enable an organization's development team to rapidly provision and run new resources, in a repeatable way that is in line with the organization's compliance requirements?

☐ Azure Policy

☐ Azure Rapid Build

■ Azure Blueprints

Explanation
Azure Blueprint will enable your development teams to define a repeatable set of Azure resources, and achieve shorter development times and faster delivery.

Multiple choice

Item 2. As the compliance admin for your organization, you need to ensure that Azure resources meet your organization's business rules? Which Azure capability should you use?

☐ Use Azure role-based access control (RBAC).

■ Use Azure Policy.

☐ Use Azure resource locks.

Explanation
Azure Policy is used to ensure that your Azure resources comply with your organization's business rules.

Multiple choice

Item 3. Which application of Microsoft Purview is used to capture metadata about enterprise data, to identify and classify sensitive data?

☐ Data Catalog.

■ Data Map.

☐ Data Estate Insights.

Explanation
Microsoft Purview Data Map is able to capture metadata about enterprise data, to identify and classify sensitive data.